

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58

Network Working Group
Request for Comments: 2002
Category: Standards Track

C. Perkins, Editor
IBK
October 1996

IP Mobility Support

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This document specifies protocol enhancements that allow transparent routing of IP datagrams to mobile nodes in the Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about its current point of attachment to the Internet. The protocol provides for registering the care-of address with a home agent. The home agent sends datagrams destined for the mobile node through a tunnel to the care-of address. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node.

Table of Contents

1. Introduction	3
1.1. Protocol Requirements	3
1.2. Goals	3
1.3. Assumptions	4
1.4. Applicability	4
1.5. New Architectural Entities	4
1.6. Terminology	5
1.7. Protocol Overview	6
1.8. Specification Language	8
1.9. Message Format and Protocol Extensibility	11
2. Agent Discovery	12
2.1. Agent Advertisement	14
2.1.1. Mobility Agent Advertisement Extension	14
2.1.2. Prefix-Lengths Extension	16
2.1.3. One-byte Padding Extension	18
2.2. Agent Solicitation	19
2.3. Foreign Agent and Home Agent Considerations	19
2.3.1. Advertised Router Addresses	20

IP Mobility Support

October 1996

2.3.2. Sequence Numbers and Rollover Handling	21
2.4. Mobile Node Considerations	21
2.4.1. Registration Required	22
2.4.2. Move Detection	22
2.4.3. Returning Home	24
2.4.4. Sequence Numbers and Rollover Handling	24
3. Registration	24
3.1. Registration Overview	24
3.2. Authentication	25
3.3. Registration Request	26
3.4. Registration Reply	29
3.5. Registration Extensions	32
3.5.1. Computing Authentication Extension Values	32
3.5.2. Mobile-Home Authentication Extension	33
3.5.3. Mobile-Foreign Authentication Extension	33
3.5.4. Foreign-Home Authentication Extension	34
3.6. Mobile Node Considerations	34
3.6.1. Sending Registration Requests	36
3.6.2. Receiving Registration Replies	40
3.6.3. Registration Retransmission	42
3.7. Foreign Agent Considerations	43
3.7.1. Configuration and Registration Tables	44
3.7.2. Receiving Registration Requests	44
3.7.3. Receiving Registration Replies	47
3.8. Home Agent Considerations	49
3.8.1. Configuration and Registration Tables	49
3.8.2. Receiving Registration Requests	49
3.8.3. Sending Registration Replies	53
4. Routing Considerations	55
4.1. Encapsulation Types	55
4.2. Unicast Datagram Routing	56
4.2.1. Mobile Node Considerations	56
4.2.2. Foreign Agent Considerations	57
4.2.3. Home Agent Considerations	58
4.3. Broadcast Datagrams	59
4.4. Multicast Datagram Routing	60
4.5. Mobile Routers	61
4.6. ARP, Proxy ARP, and Gratuitous ARP	62
5. Security Considerations	66
5.1. Message Authentication Codes	66
5.2. Areas of Security Concern in this Protocol	66
5.3. Key Management	67
5.4. Picking Good Random Numbers	67
5.5. Privacy	67
5.6. Replay Protection for Registration Requests	68
5.6.1. Replay Protection using Timestamps	68
5.6.2. Replay Protection using Nonces	69
6. Acknowledgments	71

May 13 1998 10:38:26	rfc2002.txt	Page 3
115	RFC 2002	IP Mobility Support
116		October 1996
117		
118		
119	A. Patent Issues	72
120	A.1. IBM Patent #5,159,592	72
121	A.2. IBM Patent #5,148,479	72
122	B. Link-Layer Considerations	73
123	C. TCP Considerations	73
124	C.1. TCP Timers	73
125	C.2. TCP Congestion Management	73
126	D. Example Scenarios	74
127	D.1. Registering with a Foreign Agent Care-of Address	74
128	D.2. Registering with a Co-Located Care-of Address	75
129	D.3. Deregistration	76
130	E. Applicability of Prefix Lengths Extension	76
131	Editor's Address	79
132		
133	I. Introduction	
134	IP version 4 assumes that a node's IP address uniquely identifies the	
135	node's point of attachment to the Internet. Therefore, a node must	
136	be located on the network indicated by its IP address in order to	
137	receive datagrams destined to it; otherwise, datagrams destined to	
138	the node would be undeliverable. For a node to change its point of	
139	attachment without losing its ability to communicate, currently one	
140	of the two following mechanisms must typically be employed:	
141		
142	a) the node must change its IP address whenever it changes its	
143	point of attachment, or	
144	b) host-specific routes must be propagated throughout much of	
145	the Internet routing fabric.	
146		
147	Both of these alternatives are often unacceptable. The first makes	
148	it impossible for a node to maintain transport and higher-layer	
149	connections when the node changes location. The second has obvious	
150	and severe scaling problems, especially relevant considering the	
151	explosive growth in sales of notebook (mobile) computers.	
152		
153	A new, scalable, mechanism is required for accommodating node	
154	mobility within the Internet. This document defines such a	
155	mechanism, which enables nodes to change their point of attachment to	
156	the Internet without changing their IP address.	
157		
158	1.1. Protocol Requirements	
159		
160	A mobile node must be able to communicate with other nodes after	
161	changing its link-layer point of attachment to the Internet, yet	
162	without changing its IP address.	
163		
164		
165		
166		
167		
168		
169		
170	Perkins	Standards Track
		(Page 3)

May 13 1998 10:38:26	rfc2002.txt	Page 4
171	RFC 2002	IP Mobility Support
172		October 1996
173		
174		
175	A mobile node must be able to communicate with other nodes that do	
176	not implement these mobility functions. No protocol enhancements are	
177	required in hosts or routers that are not acting as any of the new	
178	architectural entities introduced in Section 1.5.	
179		
180	All messages used to update another node as to the location of a	
181	mobile node must be authenticated in order to protect against remote	
182	redirection attacks.	
183		
184	1.2. Goals	
185		
186	The link by which a mobile node is directly attached to the Internet	
187	may often be a wireless link. This link may thus have a	
188	substantially lower bandwidth and higher error rate than traditional	
189	wired networks. Moreover, mobile nodes are likely to be battery	
190	powered, and minimizing power consumption is important. Therefore,	
191	the number of administrative messages sent over the link by which a	
192	mobile node is directly attached to the Internet should be minimized,	
193	and the size of these messages should be kept as small as is	
194	reasonably possible.	
195		
196	1.3. Assumptions	
197		
198	The protocols defined in this document place no additional	
199	constraints on the assignment of IP addresses. That is, a mobile	
200	node can be assigned an IP address by the organization that owns the	
201	machine.	
202		
203	This protocol assumes that mobile nodes will generally not change	
204	their point of attachment to the Internet more frequently than once	
205	per second.	
206		
207	This protocol assumes that IP unicast datagrams are routed based on	
208	the destination address in the datagram header (and not, for example,	
209	by source address).	
210		
211	1.4. Applicability	
212		
213	Mobile IP is intended to enable nodes to move from one IP subnet to	
214	another. It is just as suitable for mobility across homogeneous	
215	media as it is for mobility across heterogeneous media. That is,	
216	Mobile IP facilitates node movement from one Ethernet segment to	
217	another as well as it accommodates node movement from an Ethernet	
218	segment to a wireless LAN, as long as the mobile node's IP address	
219	remains the same after such a movement.	
220		
221	One can think of Mobile IP as solving the "macro" mobility management	
222	problem. It is less well suited for more "micro" mobility management	
223		
224		
225	Perkins	Standards Track
226		(Page 4)

227 RFC 2002 IP Mobility Support October 1996
228
229 applications -- for example, handoff amongst wireless transceivers,
230 each of which covers only a very small geographic area. As long as
231 node movement does not occur between points of attachment on
232 different IP subnets, link-layer mechanisms for mobility (i.e.,
233 link layer handoff) may offer faster convergence and far less
234 overhead than Mobile IP.
235
236
237 1.5. New Architectural Entities
238
239 Mobile IP introduces the following new functional entities:
240
241 Mobile Node
242
243 A host or router that changes its point of attachment from one
244 network or subnetwork to another. A mobile node may change its
245 location without changing its IP address; it may continue to
246 communicate with other Internet nodes at any location using its
247 (constant) IP address, assuming link-layer connectivity to a
248 point of attachment is available.
249
250 Home Agent
251
252 A router on a mobile node's home network which tunnels
253 datagrams for delivery to the mobile node when it is away from
254 home, and maintains current location information for the mobile
255 node.
256
257 Foreign Agent
258
259 A router on a mobile node's visited network which provides
260 routing services to the mobile node while registered. The
261 foreign agent tunnels and delivers datagrams to the mobile
262 node that were tunneled by the mobile node's home agent. For
263 datagrams sent by a mobile node, the foreign agent may serve as
264 a default router for registered mobile nodes.
265
266 A mobile node is given a long-term IP address on a home network.
267 This home address is administered in the same way as a "permanent" IP
268 address is provided to a stationary host. When away from its home
269 network, a "care-of address" is associated with the mobile node and
270 reflects the mobile node's current point of attachment. The mobile
271 node uses its home address as the source address of all IP datagrams
272 that it sends, except where otherwise described in this document for
273 datagrams sent for certain mobility management functions (e.g., as in
274 Section 3.6.1.1).
275
276
277
278
279
280
281
282

Perkins Standards Track [Page 5]

283 RFC 2002 IP Mobility Support October 1996
284
285
286 1.6. Terminology
287
288 This document frequently uses the following terms:
289
290 Agent Advertisement
291 An advertisement message constructed by attaching a
292 special Extension to a router advertisement [4] message.
293
294 Care-of Address
295 The termination point of a tunnel toward a mobile node,
296 for datagrams forwarded to the mobile node while it is
297 away from home. The protocol can use two different types
298 of care-of address: a "foreign agent care-of address" is
299 an address of a foreign agent with which the mobile node
300 is registered, and a "co-located care-of address" is an
301 externally obtained local address which the mobile node
302 has associated with one of its own network interfaces.
303
304 Correspondent Node
305 A peer with which a mobile node is communicating. A
306 correspondent node may be either mobile or stationary.
307
308 Foreign Network
309 Any network other than the mobile node's Home Network.
310
311 Home Address
312 An IP address that is assigned for an extended period of
313 time to a mobile node. It remains unchanged regardless
314 of where the node is attached to the Internet.
315
316 Home Network
317 A network, possibly virtual, having a network prefix
318 matching that of a mobile node's home address. Note that
319 standard IP routing mechanisms will deliver datagrams
320 destined to a mobile node's Home Address to the mobile
321 node's Home Network.
322
323 Link
324 A facility or medium over which nodes can communicate at
325 the link layer. A link underlies the network layer.
326
327 Link-Layer Address
328 The address used to identify an endpoint of some
329 communication over a physical link. Typically, the
330 Link-layer address is an interface's Media Access Control
331 (MAC) address.
332
333 Mobility Agent
334 Either a home agent or a foreign agent.
335
336
337
338

Perkins Standards Track [Page 6]

339 RFC 2002 IP Mobility Support October 1996
 340
 341
 342
 343 Mobility Binding
 344 The association of a home address with a care-of address,
 345 along with the remaining lifetime of that association.
 346
 347 Mobility Security Association
 348 A collection of security contexts, between a pair
 349 of nodes, which may be applied to Mobile IP protocol
 350 messages exchanged between them. Each context indicates
 351 an authentication algorithm and mode (Section 5.1), a
 352 secret (a shared key, or appropriate public/private
 353 key pair), and a style of replay protection in use
 354 (Section 5.6).
 355
 356 Node
 357 A host or a router.
 358
 359 Home
 360 A randomly chosen value, different from previous choices,
 361 inserted in a message to protect against replays.
 362
 363 Security Parameter Index (SPI)
 364 An index identifying a security context between a pair
 365 of nodes among the contexts available in the Mobility
 366 Security Association. SPI values 0 through 255 are
 367 reserved and MUST NOT be used in any Mobility Security
 368 Association.
 369
 370 Tunnel
 371 The path followed by a datagram while it is encapsulated.
 372 The model is that, while it is encapsulated, a datagram
 373 is routed to a knowledgeable decapsulating agent, which
 374 decapsulates the datagram and then correctly delivers it
 375 to its ultimate destination.
 376
 377 Virtual Network
 378 A network with no physical instantiation beyond a router
 379 (with a physical network interface on another network).
 380 The router (e.g., a home agent) generally advertises
 381 reachability to the virtual network using conventional
 382 routing protocols.
 383
 384 Visited Network
 385 A network other than a mobile node's Home Network, to
 386 which the mobile node is currently connected.
 387
 388 Visitor List
 389 The list of mobile nodes visiting a foreign agent.
 390
 391
 392
 393
 394

Perkins

Standards Track

[Page 7]

395 RFC 2002 IP Mobility Support October 1996
 396
 397
 398
 399 1.7. Protocol Overview
 400
 401 The following support services are defined for Mobile IP:
 402
 403 Agent Discovery
 404 Home agents and foreign agents may advertise their
 405 availability on each link for which they provide service.
 406 A newly arrived mobile node can send a solicitation on
 407 the link to learn if any prospective agents are present.
 408
 409 Registration
 410 When the mobile node is away from home, it registers
 411 its care-of address with its home agent. Depending on
 412 its method of attachment, the mobile node will register
 413 either directly with its home agent, or through a foreign
 414 agent which forwards the registration to the home agent.
 415
 416 The following steps provide a rough outline of operation of the
 417 Mobile IP protocol:
 418
 419 - Mobility agents (i.e., foreign agents and home agents) advertise
 420 their presence via Agent Advertisement messages (Section 2). A
 421 mobile node may optionally solicit an Agent Advertisement message
 422 from any locally attached mobility agents through an Agent
 423 Solicitation message.
 424
 425 - A mobile node receives these Agent Advertisements and determines
 426 whether it is on its home network or a foreign network.
 427
 428 - When the mobile node detects that it is located on its home
 429 network, it operates without mobility services. If returning
 430 to its home network from being registered elsewhere, the mobile
 431 node deregisters with its home agent, through exchange of a
 432 Registration Request and Registration Reply message with it.
 433
 434 - When a mobile node detects that it has moved to a foreign
 435 network, it obtains a care-of address on the foreign network.
 436 The care-of address can either be determined from a foreign
 437 agent's advertisements (a foreign agent care-of address), or by
 438 some external assignment mechanism such as DHCP [6] (a co-located
 439 care-of address).
 440
 441 - The mobile node operating away from home then registers its
 442 new care-of address with its home agent through exchange of a
 443 Registration Request and Registration Reply message with it,
 444 possibly via a foreign agent (Section 3).
 445
 446
 447
 448
 449
 450

Perkins

Standards Track

[Page 8]

451 RFC 2002 IP Mobility Support October 1996

452

453

454

455

456 Datagrams sent to the mobile node's home address are intercepted

457 by its home agent, tunneled by the home agent to the mobile

458 node's care-of address, received at the tunnel endpoint (either

459 at a foreign agent or at the mobile node itself), and finally

460 delivered to the mobile node (Section 4.2.3).

461

462 In the reverse direction, datagrams sent by the mobile node

463 are generally delivered to their destination using standard IP

464 routing mechanisms, not necessarily passing through the home

465 agent.

466

467 When away from home, Mobile IP uses protocol tunneling to hide a

468 mobile node's home address from intervening routers between its home

469 network and its current location. The tunnel terminates at the

470 mobile node's care-of address. The care-of address must be an

471 address to which datagrams can be delivered via conventional IP

472 routing. At the care-of address, the original datagram is removed

473 from the tunnel and delivered to the mobile node.

474

475 Mobile IP provides two alternative modes for the acquisition of a

476 care-of address:

477

478 - A "foreign agent care-of address" is a care-of address provided

479 by a foreign agent through its Agent Advertisement messages. In

480 this case, the care-of address is an IP address of the foreign

481 agent. In this mode, the foreign agent is the endpoint of the

482 tunnel and, upon receiving tunneled datagrams, decapsulates them

483 and delivers the inner datagram to the mobile node. This mode

484 of acquisition is preferred because it allows many mobile nodes

485 to share the same care-of address and therefore does not place

486 unnecessary demands on the already limited IPv4 address space.

487

488 - A "co-located care-of address" is a care-of address acquired

489 by the mobile node as a local IP address through some external

490 means, which the mobile node then associates with one of its own

491 network interfaces. The address may be dynamically acquired as

492 a temporary address by the mobile node such as through DHCP [6],

493 or may be owned by the mobile node as a long-term address for its

494 use only while visiting some foreign network. Specific external

495 methods of acquiring a local IP address for use as a co-located

496 care-of address are beyond the scope of this document. When

497 using a co-located care-of address, the mobile node serves as the

498 endpoint of the tunnel and itself performs decapsulation of the

499 datagrams tunneled to it.

500

501 The mode of using a co-located care-of address has the advantage that

502 it allows a mobile node to function without a foreign agent. For

503 example, in networks that have not yet deployed a foreign agent,

504

505

506 Perkins Standards Track [Page 9]

507 RFC 2002 IP Mobility Support October 1996

508

509

510

511 It does, however, place additional burden on the IPv4 address space

512 because it requires a pool of addresses within the foreign network to

513 be made available to visiting mobile nodes. It is difficult to

514 efficiently maintain pools of addresses for each subnet that may

515 permit mobile nodes to visit.

516

517 It is important to understand the distinction between the care-of

518 address and the foreign agent functions. The care-of address is

519 simply the endpoint of the tunnel. It might indeed be an address of

520 a foreign agent (a foreign agent care-of address), but it might

521 instead be an address temporarily acquired by the mobile node (a co-

522 located care-of address). A foreign agent, on the other hand, is a

523 mobility agent that provides services to mobile nodes. See Sections

524 3.7 and 4.2.2 for additional details.

525

526 A home agent MUST be able to attract and intercept datagrams that are

527 destined to the home address of any of its registered mobile nodes.

528 Using the proxy and gratuitous ARP mechanisms described in Section

529 4.6, this requirement can be satisfied if the home agent has a

530 network interface on the link indicated by the mobile node's home

531 address. Other placements of the home agent relative to the mobile

532 node's home location MAY also be possible using other mechanisms for

533 intercepting datagrams destined to the mobile node's home address.

534 Such placements are beyond the scope of this document.

535

536 Similarly, a mobile node and a prospective or current foreign agent

537 MUST be able to exchange datagrams without relying on standard IP

538 routing mechanisms; that is, those mechanisms which make forwarding

539 decisions based upon the network-prefix of the destination address in

540 the IP header. This requirement can be satisfied if the foreign

541 agent and the visiting mobile node have an interface on the same

542 link. In this case, the mobile node and foreign agent simply bypass

543 their normal IP routing mechanism when sending datagrams to each

544 other, addressing the underlying link-layer packets to their

545 respective link-layer addresses. Other placements of the foreign

546 agent relative to the mobile node MAY also be possible using other

547 mechanisms to exchange datagrams between these nodes, but such

548 placements are beyond the scope of this document.

549

550 If a mobile node is using a co-located care-of address (as described

551 in (b) above), the mobile node MUST be located on the link identified

552 by the network prefix of this care-of address. Otherwise, datagrams

553 destined to the care-of address would be undeliverable.

554

555 For example, the figure below illustrates the routing of datagrams to

556 and from a mobile node away from home, once the mobile node has

557 registered with its home agent. In the figure below, the mobile node

558 is using a foreign agent care-of address:

559

560

561

562 Perkins Standards Track [Page 10]

563 RFC 2002 IP Mobility Support October 1996

564

565

566

567

568 2) Datagram is intercepted 3) Datagram is

569 by home agent and detunneled and

570 is tunneled to the delivered to the

571 care-of address. mobile node.

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

1) Datagram to mobile node arrives on home network via standard IP routing.

2) For datagrams sent by the mobile node, standard IP routing delivers each to its destination. In this figure, the foreign agent is the mobile node's default router.

3) Specification Language

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

MUST This word, or the adjective "required", means that the definition is an absolute requirement of the specification.

MUST NOT This phrase means that the definition is an absolute prohibition of the specification.

SHOULD This word, or the adjective "recommended", means that, in some circumstances, valid reasons may exist to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course. Unexpected results may result otherwise.

MAY This word, or the adjective "optional", means that this item is one of an allowed set of alternatives. An implementation which does not include this option MUST be prepared to interoperate with another implementation which does include the option.

Perkins Standards Track [Page 11]

619 RFC 2002 IP Mobility Support October 1996

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

silently discard

The implementation discards the datagram without further processing, and without indicating an error to the sender. The implementation SHOULD provide the capability of logging the error, including the contents of the discarded datagram, and SHOULD record the event in a statistics counter.

1.9. Message Format and Protocol Extensibility

Mobile IP defines a set of new control messages, sent with UDP [17] using well-known port number 434. Currently, the following two message types are defined:

1 Registration Request

3 Registration Reply

Up-to-date values for the message types for Mobile IP control messages are specified in the most recent "Assigned Numbers" [20].

In addition, for Agent Discovery, Mobile IP makes use of the existing Router Advertisement and Router Solicitation messages defined for ICMP Router Discovery [4].

Mobile IP defines a general Extension mechanism to allow optional information to be carried by Mobile IP control messages or by ICMP Router Discovery messages. Each of these Extensions (with one exception) is encoded in the following Type-Length-Value format:

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2

Type Length Data

Type Indicates the particular type of Extension.

Length Indicates the length (in bytes) of the data field within this Extension. The length does NOT include the Type and Length bytes.

Data The particular data associated with this Extension. This field may be zero or more bytes in length. The format and length of the data field is determined by the type and length fields.

Perkins Standards Track [Page 12]

575
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730

RFC 2002

IP Mobility Support.

October 1996

Extensions allow variable amounts of information to be carried within each datagram. The end of the list of Extensions is indicated by the total length of the IP datagram.

Two separately maintained sets of numbering spaces, from which Extension Type values are allocated, are used in Mobile IP:

- The first set consists of those Extensions which may appear only in Mobile IP control messages (those sent to and from UDP port number 434). Currently, the following Types are defined for Extensions appearing in Mobile IP control messages:
 - 32 Mobile-Home Authentication
 - 33 Mobile-Foreign Authentication
 - 34 Foreign-Home Authentication
- The second set consists of those extensions which may appear only in ICMP Router Discovery messages (4). Currently, Mobile IP defines the following Types for Extensions appearing in ICMP Router Discovery messages:
 - 0 One-byte Padding (encoded with no Length nor Data field)
 - 16 Mobility Agent Advertisement
 - 19 Prefix-Lengths

Each individual Extension is described in detail in a separate section later in this document. Up-to-date values for these Extension Type numbers are specified in the most recent "Assigned Numbers" [20].

Due to the separation (orthogonality) of these sets, it is conceivable that two Extensions that are defined at a later date could have identical Type values, so long as one of the Extensions may be used only in Mobile IP control messages and the other may be used only in ICMP Router Discovery messages.

When an Extension numbered in either of these sets within the range 0 through 127 is encountered but not recognized, the message containing that Extension MUST be silently discarded. When an Extension numbered in the range 128 through 255 is encountered which is not recognized, that particular Extension is ignored, but the rest of the Extensions and message data MUST still be processed. The Length field of the Extension is used to skip the Data field in searching for the next Extension.

Perkins

Standards Track

[Page 13]

731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786

RFC 2002

IP Mobility Support

October 1996

2. Agent Discovery

Agent Discovery is the method by which a mobile node determines whether it is currently connected to its home network or to a foreign network, and by which a mobile node can detect when it has moved from one network to another. When connected to a foreign network, the methods specified in this section also allow the mobile node to determine the foreign agent care-of address being offered by each foreign agent on that network.

Mobile IP extends ICMP Router Discovery [4] as its primary mechanism for Agent Discovery. An Agent Advertisement is formed by including a Mobility Agent Advertisement Extension in an ICMP Router Advertisement message (Section 2.1). An Agent Solicitation message is identical to an ICMP Router Solicitation, except that its IP TTL MUST be set to 1 (Section 2.2). This section describes the message formats and procedures by which mobile nodes, foreign agents, and home agents cooperate to realize Agent Discovery.

Agent Advertisement and Agent Solicitation may not be necessary for link layers that already provide this functionality. The method by which mobile nodes establish link-layer connections with prospective agents is outside the scope of this document (but see Appendix B). The procedures described below assume that such link-layer connectivity has already been established.

No authentication is required for Agent Advertisement and Agent Solicitation messages. They MAY be authenticated using the IP Authentication Header [1], which is unrelated to the messages described in this document. Further specification of the way in which Advertisement and Solicitation messages may be authenticated is outside of the scope of this document.

2.1. Agent Advertisement

Agent Advertisements are transmitted by a mobility agent to advertise its services on a link. Mobile nodes use these advertisements to determine their current point of attachment to the Internet. An Agent Advertisement is an ICMP Router Advertisement that has been extended to also carry an Mobility Agent Advertisement Extension (Section 2.1.1) and, optionally, a Prefix-Lengths Extension (Section 2.1.2). One-byte Padding Extension (Section 2.1.3), or other Extensions that might be defined in the future.

Within an Agent Advertisement message, ICMP Router Advertisement fields of the message are required to conform to the following additional specifications:

Perkins

Standards Track

[Page 14]

78 / IP Mobility Support October 1996

- Link-Layer Fields

Destination Address

The link-layer destination address of a unicast Agent Advertisement MUST be the same as the source link-layer address of the Agent Solicitation which prompted the Advertisement.

66L
IP Fields

```

801 TTL The TTL for all Agent Advertisements MUST be set
802 to 1.

```

Destination Address

As specified for ICMP Router Discovery [4], the IP destination address of an Agent Advertisement MUST be either the "all systems on this link" multicast address (224.0.0.1) [5] or the "limited broadcast" address (255.255.255.255). The subnet-directed broadcast address of the form <prefix>.<1> cannot be used since mobile nodes will not generally know the prefix of the foreign network.

ICMP Fields

Code
816
817

The Code field of the agent advertisement is interpreted as follows:

```

0 The mobility agent handles common traffic -- that
  is, it acts as a router for IP datagrams not
  necessarily related to mobile nodes.
16 The mobility agent does not route common traffic.
  However, all foreign agents MUST (minimally)
  forward to a default router any datagrams received
  from a registered mobile node (Section 4.2.2).

```

827 Lifetime

The maximum length of time that the Advertisement is considered valid in the absence of further Advertisements.

Router Address(es)

See Section 2.3.1 for a discussion of the addresses that may appear in this portion of the Agent Advertisement.

Perkins

342 Perkins Standards Track

442 Perkins Standards Track

43		
44	RFC 2002	IP Mobility Support
		October 1996

47 Num Addr

The number of Router Addresses advertised in this message. Note that in an Agent Advertisement message, the number of router addresses specified in the ICMP Router Advertisement portion of the message MAY be set to 0. See Section 2.3.1 for details.

54 If sent periodically, the nominal interval at which Agent
55 Advertisements are sent SHOULD be 1/3 of the advertisement Lifetime
56 given in the ICMP header. This allows a mobile node to miss three
57 successive advertisements before deleting the agent from its list of
58 valid agents. The actual transmission time for each advertisement
59 SHOULD be slightly randomized [4] in order to avoid synchronization
60 and subsequent collisions with other Agent Advertisements that may be
61 sent by other agents (or with other Router Advertisements sent by
62 other routers). Note that this field has no relation to the
63 "Registration Lifetime" field within the Mobility Agent Advertisement
64 Extension defined below.

2.1.1.1. Mobility Agent Advertisement Extension

The Mobility Agent Advertisement Extension follows the ICMP Router Advertisement fields. It is used to indicate that an ICMP Router Advertisement message is also an Agent Advertisement being sent by a mobility agent. The Mobility Agent Advertisement Extension is defined as follows:

[illegible]

Type	16
34	16

Length $(6 + 4 \cdot N)$, where N is the number of care-of addresses advertised.

Sequence Number

00 The count of Agent Advertisement messages sent since the
11 agent was initialized (Section 2.3.2).

Subj: 268

Standards Track	Standards Track
898 Perkins	898 Perkins

Standards Track	898	Standards Track
(Page 15)		(Page 16)

899 RFC 2002 IP Mobility Support October 1996
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954

Registration Lifetime
The longest lifetime (measured in seconds) that this agent is willing to accept in any Registration Request. A value of 0xffff indicates infinity. This field has no relation to the "lifetime" field within the ICMP Router Advertisement portion of the Agent Advertisement.

R Registration required. Registration with this foreign agent for another foreign agent on this link is required rather than using a co-located care-of address.

B Busy. The foreign agent will not accept registrations from additional mobile nodes.

H Home agent. This agent offers service as a home agent on the link on which this Agent Advertisement message is sent.

F Foreign agent. This agent offers service as a foreign agent on the link on which this Agent Advertisement message is sent.

H Minimal encapsulation. This agent implements receiving tunneled datagrams that use minimal encapsulation [15].

G GRE encapsulation. This agent implements receiving tunneled datagrams that use GRE encapsulation [8].

V Van Jacobson header compression. This agent supports use of Van Jacobson header compression [10] over the link with any registered mobile node.

reserved Sent as zero; ignored on reception.

Care-of Address(es)
The advertised foreign agent care-of address(es) provided by this foreign agent. An Agent Advertisement MUST include at least one care-of address if the 'F' bit is set. The number of care-of addresses present is determined by the Length field in the Extension.

A home agent MUST always be prepared to serve the mobile nodes for which it is the home agent. A foreign agent may at times be too busy to serve additional mobile nodes; even so, it must continue to send Agent Advertisements, so that any mobile nodes already registered with it will know that they have not moved out of range of the foreign agent and that the foreign agent has not failed. A foreign

Perkins Standards Track (Page 17)

955 RFC 2002 IP Mobility Support October 1996
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010

agent may indicate that it is "too busy" to allow new mobile nodes to register with it. By setting the 'B' bit in its Agent Advertisements, an Agent Advertisement message MUST NOT have the 'B' bit set if the 'F' bit is not also set, and at least one of the 'F' bit and the 'H' bit MUST be set in any Agent Advertisement message sent.

When a foreign agent wishes to require registration even from those mobile nodes which have acquired a co-located care-of address, it sets the 'R' bit to one. Because this bit applies only to foreign agents, an agent MUST NOT set the 'R' bit to one unless the 'F' bit is also set to one.

2.1.2. Prefix-Lengths Extension

The Prefix-Lengths Extension MAY follow the Mobility Agent Advertisement Extension. It is used to indicate the number of bits of network prefix that applies to each Router Address listed in the ICMP Router Advertisement portion of the Agent Advertisement. Note that the prefix lengths given DO NOT apply to care-of addresses listed in the Mobility Agent Advertisement Extension. The Prefix-Lengths Extension is defined as follows:

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Type | Length | Prefix Length | ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

Type 19 (Prefix-Lengths Extension)

Length N, where N is the value of the Num Adrs field in the ICMP Router Advertisement portion of the Agent Advertisement.

Prefix Length(s)
The number of leading bits that define the network number of the corresponding Router Address listed in the ICMP Router Advertisement portion of the message. The prefix length for each Router Address is encoded as a separate byte, in the order that the Router Addresses are listed in the ICMP Router Advertisement portion of the message.

See Section 2.4.2 for information about how the Prefix Lengths Extension MAY be used by a mobile node when determining whether it has moved. See Appendix E for implementation details about the use of this Extension.

Perkins Standards Track (Page 18)

1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066

RFC 2002 IP Mobility Support October 1996

2.1.3. One-byte Padding Extension

Some IP protocol implementations insist upon padding ICMP messages to an even number of bytes. If the ICMP length of an Agent Advertisement is odd, this Extension MAY be included in order to make the ICMP length even. Note that this Extension is NOT intended to be a general-purpose Extension to be included in order to word- or long-align the various fields of the Agent Advertisement. An Agent Advertisement SHOULD NOT include more than one One-byte Padding Extension and if present, this Extension SHOULD be the last Extension in the Agent Advertisement.

Note that unlike other Extensions used in Mobile IP, the One-byte Padding Extension is encoded as a single byte, with no "Length" nor "Data" field present. The One-byte Padding Extension is defined as follows:

```

0 1 2 3 4 5 6 7
+---+---+---+---+
|   Type   |
+---+---+---+---+

```

Type 0 (One-byte Padding Extension)

2.2. Agent Solicitation

An Agent Solicitation is identical to an ICMP Router Solicitation with the further restriction that the IP TTL Field MUST be set to 1.

2.3. Foreign Agent and Home Agent Considerations

Any mobility agent which cannot be discovered by a link-layer protocol MUST send Agent Advertisements. An agent which can be discovered by a link-layer protocol SHOULD also implement Agent Advertisements. However, the Advertisements need not be sent, except when the site policy requires registration with the agent (i.e., when the 'R' bit is set), or as a response to a specific Agent Solicitation. All mobility agents SHOULD respond to Agent Solicitations.

The same procedures, defaults, and constants are used in Agent Advertisement messages and Agent Solicitation messages as specified for ICMP Router Discovery [4], except that:

- a mobility agent MUST limit the rate at which it sends broadcast or multicast Agent Advertisements; a recommended maximum rate is once per second, AND

1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122

RFC 2002 IP Mobility Support October 1996

- a mobility agent that receives a Router Solicitation MUST NOT require that the IP Source Address is the address of a neighbor (i.e., an address that matches one of the router's own addresses on the arrival interface, under the subnet mask associated with that address of the router).
- a mobility agent MAY be configured to send Agent Advertisements only in response to an Agent Solicitation message.

If the home network is not a virtual network, then the home agent for any mobile node SHOULD be located on the link identified by the mobile node's home address, and Agent Advertisement messages sent by the home agent on this link MUST have the 'H' bit set. In this way, mobile nodes on their own home network will be able to determine that they are indeed at home. Any Agent Advertisement messages sent by the home agent on another link to which it may be attached (if it is a mobility agent serving more than one link), MUST NOT have the 'H' bit set, unless the home agent also serves as a home agent (to other mobile nodes) on that other link.

If the home network is a virtual network, the home network has no physical realization external to the home agent itself. In this case, there is no physical network link on which to send Agent Advertisement messages advertising the home agent. Mobile nodes for which this is the home network are always treated as being away from home.

On a particular subnet, either all mobility agents MUST include the Prefix-Lengths Extension or all of them MUST NOT include this Extension. Equivalently, it is prohibited for some agents on a given subnet to include the Extension but for others not to include it. Otherwise, one of the move detection algorithms designed for mobile nodes will not function properly (Section 2.4.2).

2.3.1. Advertised Router Addresses

The ICMP Router Advertisement portion of the Agent Advertisement MAY contain one or more router addresses. Thus, an agent MAY include one of its own addresses in the advertisement. A foreign agent MAY discourage use of this address as a default router by setting the preference to a low value and by including the address of another router in the advertisement (with a correspondingly higher preference). Nevertheless, a foreign agent MUST route datagrams it receives from registered mobile nodes (Section 4.2.2).

May 13 1998 10:38:26			rfc2002.txt	Page 21
1124	RFC 2002	IP Mobility Support		
1125				October 1996
1126				
1127	2.3.2. Sequence Numbers and Rollover Handling			
1128	The sequence number in Agent Advertisements ranges from 0 to 0xffff.			
1129	After booting, an agent MUST use the number 0 for its first			
1130	advertisement. Each subsequent advertisement MUST use the sequence			
1131	number one greater, with the exception that the sequence number			
1132	0xffff MUST be followed by sequence number 256. In this way, mobile			
1133	nodes can distinguish reductions in sequence numbers that result from			
1134	reboots, from reductions that result in rollover of the sequence			
1135	number after it attains the value 0xffff.			
1136				
1137				
1138	2.4. Mobile Node Considerations			
1139				
1140	Every mobile node MUST implement Agent Solicitation. Solicitations			
1141	SHOULD only be sent in the absence of Agent Advertisements and when a			
1142	care of address has not been determined through a link-layer protocol			
1143	or other means. The mobile node uses the same procedures, defaults,			
1144	and constants for Agent Solicitation as specified for ICMP Router			
1145	Solicitation messages [4], except that the mobile node MAY solicit			
1146	more often than once every three seconds, and that a mobile node that			
1147	is currently not connected to any foreign agent MAY solicit more			
1148	times than MAX_SOLICITATIONS.			
1149				
1150	The rate at which a mobile node sends Solicitations MUST be limited			
1151	by the mobile node. The mobile node MAY send three initial			
1152	Solicitations at a maximum rate of one per second while searching for			
1153	an agent. After this, the rate at which Solicitations are sent MUST			
1154	be reduced so as to limit the overhead on the local link. Subsequent			
1155	Solicitations MUST be sent using a binary exponential backoff			
1156	mechanism, doubling the interval between consecutive Solicitations,			
1157	up to a maximum interval. The maximum interval SHOULD be chosen			
1158	appropriately based upon the characteristics of the media over which			
1159	the mobile node is soliciting. This maximum interval SHOULD be at			
1160	least one minute between Solicitations.			
1161				
1162	While still searching for an agent, the mobile node MUST NOT increase			
1163	the rate at which it sends Solicitations unless it has received a			
1164	positive indication that it has moved to a new link. After			
1165	successfully registering with an agent, the mobile node SHOULD also			
1166	increase the rate at which it will send Solicitations when it next			
1167	begins searching for a new agent with which to register. The			
1168	increased solicitation rate MAY revert to the maximum rate, but then			
1169	MUST be limited in the manner described above. In all cases, the			
1170	recommended solicitation intervals are nominal values. Mobile nodes			
1171	MUST randomize their solicitation times around these nominal values			
1172	as specified for ICMP Router Discovery [4].			
1173				
1174				
1175				
1176				
1177				
1178	Perkins	Standards Track		(Page 21)

May 13 1998 10:38:26			rfc2002.txt	Page 22
1179	RFC 2002	IP Mobility Support		October 1996
1180				
1181				
1182	Mobile nodes MUST process received Agent Advertisements. A mobile			
1183	node can distinguish an Agent Advertisement message from other uses			
1184	of the ICMP Router Advertisement message by examining the number of			
1185	advertised addresses and the IP Total Length field. When the IP			
1186	total length indicates that the ICMP message is longer than needed			
1187	for the number of advertised addresses, the remaining data is			
1188	interpreted as one or more Extensions. The presence of a Mobility			
1189	Agent Advertisement Extension identifies the advertisement as an			
1190	Agent Advertisement.			
1191				
1192				
1193	When multiple methods of agent discovery are in use, the mobile node			
1194	SHOULD first attempt registration with agents including Mobility			
1195	Agent Advertisement Extensions in their advertisements, in preference			
1196	to those discovered by other means. This preference maximizes the			
1197	likelihood that the registration will be recognized, thereby			
1198	minimizing the number of registration attempts.			
1199				
1200	2.4.1. Registration Required			
1201				
1202	When the mobile node receives an Agent Advertisement with the 'R' bit			
1203	set, the mobile node SHOULD register through the foreign agent, even			
1204	when the mobile node might be able to acquire its own co-located			
1205	care-of address. This feature is intended to allow sites to enforce			
1206	visiting policies (such as accounting) which require exchanges of			
1207	authorization.			
1208				
1209	2.4.2. Move Detection			
1210				
1211	Two primary mechanisms are provided for mobile nodes to detect when			
1212	they have moved from one subnet to another. Other mechanisms MAY			
1213	also be used. When the mobile node detects that it has moved, it			
1214	SHOULD register (Section 3) with a suitable care-of address on the			
1215	new foreign network. However, the mobile node MUST NOT register more			
1216	frequently than once per second on average, as specified in Section			
1217	3.6.3.			
1218				
1219				
1220				
1221				
1222				
1223				
1224				
1225				
1226				
1227				
1228				
1229				
1230				
1231				
1232				
1233				
1234	Perkins	Standards Track		(Page 22)

May 13 1998 10:38:26	rfc2002.txt	Page 23
1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290	<p>RFC 2002</p> <p>IP Mobility Support</p> <p>October 1996</p> <p>2.4.2.1. Algorithm 1</p> <p>The first method of move detection is based upon the Lifetime field within the main body of the ICMP Router Advertisement portion of the Agent Advertisement. A mobile node SHOULD record the Lifetime received in any Agent Advertisements, until that Lifetime expires. If the mobile node fails to receive another advertisement from the same agent within the specified Lifetime, it SHOULD assume that it has lost contact with that agent. If the mobile node has previously received an Agent Advertisement from another agent for which the Lifetime field has not yet expired, the mobile node MAY immediately attempt registration with that other agent. Otherwise, the mobile node SHOULD attempt to discover a new agent with which to register.</p> <p>2.4.2.2. Algorithm 2</p> <p>The second method uses network prefixes. The Prefix-Lengths Extension MAY be used in some cases by a mobile node to determine whether or not a newly received Agent Advertisement was received on the same subnet as the mobile node's current care-of address. If the prefixes differ, the mobile node MAY assume that it has moved. If a mobile node is currently using a foreign agent care-of address, the mobile node SHOULD NOT use this method of move detection unless both the current agent and the new agent include the Prefix-Lengths Extension in their respective Agent Advertisements; if this Extension is missing from one or both of the advertisements, this method of move detection SHOULD NOT be used. Similarly, if a mobile node is using a co-located care-of address, it SHOULD not use this method of move detection unless the new agent includes the Prefix-Lengths Extension in its Advertisement and the mobile node knows the network prefix of its current co-located care-of address. On the expiration of its current registration, if this method indicates that the mobile node has moved, rather than re-registering with its current care-of address, a mobile node MAY choose instead to register with a the foreign agent sending the new Advertisement with the different network prefix. The Agent Advertisement with the different registration is based MUST NOT have expired according to its Lifetime field.</p>	
Perkins	Standards Track	[Page 23]

May 13 1998 10:38:26	rfc2002.txt	Page 24
1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346	<p>RFC 2002</p> <p>IP Mobility Support</p> <p>October 1996</p> <p>2.4.3. Returning Home</p> <p>A mobile node can detect that it has returned to its home network when it receives an Agent Advertisement from its own home agent. If so, it SHOULD deregister with its home agent (Section 3). Before attempting to deregister, the mobile node SHOULD configure its routing table appropriately for its home network (Section 4.2.1). In addition, if the home network is using ARP [16], the mobile node MUST follow the procedures described in Section 4.6 with regard to ARP, proxy ARP, and gratuitous ARP.</p> <p>2.4.4. Sequence Numbers and Rollover Handling</p> <p>If a mobile node detects two successive values of the sequence number in the Agent Advertisements from the foreign agent with which it is registered, the second of which is less than the first and inside the range 0 to 255, the mobile node SHOULD register again. If the second value is less than the first but is greater than or equal to 256, the mobile node SHOULD assume that the sequence number has rolled over past its maximum value (0xffff), and that reregistration is not necessary (Section 2.3).</p> <p>3. Registration</p> <p>Mobile IP registration provides a flexible mechanism for mobile nodes to communicate their current reachability information to their home agent. It is the method by which mobile nodes:</p> <ul style="list-style-type: none"> - request forwarding services when visiting a foreign network, - inform their home agent of their current care-of address, - renew a registration which is due to expire, and/or - deregister when they return home. <p>Registration messages exchange information between a mobile node, (optionally) a foreign agent, and the home agent. Registration creates or modifies a mobility binding at the home agent, associating the mobile node's home address with its care-of address for the specified Lifetime.</p>	
Perkins	Standards Track	[Page 24]

1347 RFC 2002 IP Mobility Support October 1996

1348 Several other (optional) capabilities are available through the

1349 registration procedure, which enable a mobile node to:

1350 maintain multiple simultaneous registrations, so that a copy of

1351 each datagram will be tunneled to each active care-of address

1352 - deregister specific care-of addresses while retaining other

1353 mobility bindings, and

1354 discover the address of a home agent if the mobile node is not

1355 configured with this information.

1356 3.1. Registration Overview

1357 Mobile IP defines two different registration procedures, one via a

1358 foreign agent that relays the registration to the mobile node's home

1359 agent, and one directly with the mobile node's home agent. The

1360 following rules determine which of these two registration procedures

1361 to use in any particular circumstance:

1362 If a mobile node is registering a foreign agent care-of address,

1363 the mobile node MUST register via that foreign agent.

1364 If a mobile node is using a co-located care-of address, and

1365 receives an Agent Advertisement from a foreign agent on the

1366 link on which it is using this care-of address, the mobile node

1367 SHOULD register via that foreign agent (or via another foreign

1368 agent on this link) if the 'R' bit is set in the received Agent

1369 Advertisement message.

1370 If a mobile node is otherwise using a co-located care-of address,

1371 the mobile node MUST register directly with its home agent.

1372 If a mobile node has returned to its home network and is

1373 (de)registering with its home agent, the mobile node MUST

1374 register directly with its home agent.

1375 Both registration procedures involve the exchange of Registration

1376 Request and Registration Reply messages (Sections 3.3 and 3.4). When

1377 registering via a foreign agent, the registration procedure requires

1378 the following four messages:

1379 a) The mobile node sends a Registration Request to the

1380 prospective foreign agent to begin the registration process.

1381 b) The foreign agent processes the Registration Request and then

1382 relays it to the home agent.

1383 Perkins

Standards Track

(Page 25)

1403 RFC 2002 IP Mobility Support October 1996

1404 c) The home agent sends a Registration Reply to the foreign

1405 agent to grant or deny the Request.

1406 d) The foreign agent processes the Registration Reply and then

1407 relays it to the mobile node to inform it of the disposition

1408 of its Request.

1409 When the mobile node instead registers directly with its home agent,

1410 the registration procedure requires only the following two messages:

1411 a) The mobile node sends a Registration Request to the home

1412 agent.

1413 b) The home agent sends a Registration Reply to the mobile

1414 node, granting or denying the Request.

1415 The registration messages defined in Sections 3.3 and 3.4 use the

1416 User Datagram Protocol (UDP) [17]. A nonzero UDP checksum SHOULD be

1417 included in the header, and MUST be checked by the recipient.

1418 3.2. Authentication

1419 Each mobile node, foreign agent, and home agent MUST be able to

1420 support a mobility security association for mobile entities, indexed

1421 by their SPI and IP address. In the case of the mobile node, this

1422 must be its Home Address. See Section 5.1 for requirements for

1423 support of authentication algorithms. Registration messages between

1424 a mobile node and its home agent MUST be authenticated with the

1425 Mobile-Home Authentication Extension (Section 3.5.2). This Extension

1426 immediately follows all non-authentication Extensions, except those

1427 foreign agent-specific Extensions which may be added to the message

1428 after the mobile node computes the authentication.

1429 3.3. Registration Request

1430 A mobile node registers with its home agent using a Registration

1431 Request message so that its home agent can create or modify a

1432 mobility binding for that mobile node (e.g., with a new lifetime).

1433 The Request may be relayed to the home agent by the foreign agent

1434 through which the mobile node is registering, or it may be sent

1435 directly to the home agent in the case in which the mobile node is

1436 registering a co-located care-of address.

1437 IP fields:

1438 Source Address Typically the interface address from which the

1439 message is sent.

1440 Perkins

Standards Track

(Page 26)

May 13 1998 10:38:26		rfc2002.txt		Page 27
1452	RFC 2002	IP Mobility Support	October 1996	
1461				
1462				
1463		Destination Address Typically that of the foreign agent or the		
1464		home agent.		
1465				
1466		See Sections 3.6.1.1 and 3.7.2.2 for details.		
1467				
1468		UDP fields:		
1469				
1470		Source Port	variable	
1471		Destination Port	434	
1472				
1473				
1474		The UDP header is followed by the Mobile IP fields shown below:		
1475				
1476				
1477				
1478				
1479				
1480		Type	[S][B][M][G][V][Lsv]	Lifetime
1481				
1482			Home Address	
1483			Home Agent	
1484			Care-of Address	
1485				
1486			Identification	
1487				
1488				
1489				
1490				
1491		Extensions		
1492				
1493				
1494				
1495		Type	1 (Registration Request)	
1496				
1497		S	Simultaneous bindings. If the 'S' bit is set, the mobile	
1498			node is requesting that the home agent retain its prior	
1499			mobility bindings, as described in Section 3.6.1.2.	
1500		R	Broadcast datagrams. If the 'B' bit is set, the mobile	
1501			node requests that the home agent tunnel to it any	
1502			broadcast datagrams that it receives on the home network,	
1503			as described in Section 4.3.	
1504				
1505		B	Decapsulation by mobile node. If the 'B' bit is set, the	
1506			mobile node will itself decapsulate datagrams which are	
1507			sent to the care-of address. That is, the mobile node is	
1508			using a co-located care-of address.	
1509				
1510				
1511				
1512				
1513				
1514	Perkins		Standards Track	(Page 27)

May 13 1998 10:38:26		rfc2002.txt		Page 28
1515	RFC 2002	IP Mobility Support	October 1996	
1516				
1517				
1518				
1519	M			
1520		Minimal encapsulation. If the 'N' bit is set, the		
1521		mobile node requests that its home agent use minimal		
1522		encapsulation [15] for datagrams tunneled to the mobile		
1523		node.		
1524	G			
1525		GRE encapsulation. If the 'G' bit is set, the		
1526		mobile node requests that its home agent use GRE		
1527		encapsulation [8] for datagrams tunneled to the mobile		
1528		node.		
1529	V			
1530		The mobile node requests that its mobility agent use Van		
1531		Jacobson header compression [10] over its link with the		
1532		mobile node.		
1533	rsv	Reserved bits; sent as zero		
1534				
1535	Lifetime			
1536		The number of seconds remaining before the registration		
1537		is considered expired. A value of zero indicates a		
1538		request for deregistration. A value of 0xffff indicates		
1539		infinity.		
1540				
1541	Home Address			
1542		The IP address of the mobile node.		
1543				
1544	Home Agent			
1545		The IP address of the mobile node's home agent.		
1546				
1547	Care-of Address			
1548		The IP address for the end of the tunnel.		
1549				
1550	Identification			
1551		A 64-bit number, constructed by the mobile node, used for		
1552		matching Registration Requests with Registration Replies,		
1553		and for protecting against replay attacks of registration		
1554		messages. See Sections 5.4 and 5.6.		
1555				
1556	Extensions			
1557		The fixed portion of the Registration Request is followed		
1558		by one or more of the Extensions listed in Section 3.5.		
1559		The Mobile-Home Authentication Extension MUST be included		
1560		in all Registration Requests. See Sections 3.6.1.3		
1561		and 3.7.2.2 for information on the relative order in		
1562		which different extensions, when present, MUST be placed		
1563		in a Registration Request message.		
1564				
1565				
1566				
1567				
1568				
1569	Perkins		Standards Track	(Page 28)
1570				

1571 RFC 2002 IP Mobility Support October 1996

1572

1573

1574

1575

1576

1577

1578

1579

1580

1581

1582

1583

1584

1585

1586

1587

1588

1589

1590

1591

1592

1593

1594

1595

1596

1597

1598

1599

1600

1601

1602

1603

1604

1605

1606

1607

1608

1609

1610

1611

1612

1613

1614

1615

1616

1617

1618

1619

1620

1621

1622

1623

1624

1625

1626

Perkins

Standards Track

(Page 29)

4.4. Registration Reply

A mobility agent returns a Registration Reply message to a mobile node which has sent a Registration Request (Section 3.1) message. If the mobile node is requesting services from a foreign agent, that foreign agent will receive the Reply from the home agent and subsequently relay it to the mobile node. The Reply message contains the necessary codes to inform the mobile node about the status of its Request, along with the lifetime granted by the home agent, which MAY be smaller than the original Request.

The foreign agent MUST NOT increase the Lifetime selected by the mobile node in the Registration Request, since the Lifetime is covered by the Mobile-Inne Authentication Extension, which cannot be increase the lifetime selected by the foreign agent. The home agent MUST NOT increase the lifetime selected by the mobile node in the Registration Request, since doing so could increase it beyond the maximum Registration lifetime allowed by the foreign agent. If the Lifetime received in the Registration Reply is greater than that in the Registration Request, the Lifetime in the Request MUST be used. When the Lifetime received in the Registration Reply is less than that in the Registration Request, the Lifetime in the Reply MUST be used.

IP fields:

Source Address

Typically copied from the destination address of the Registration Request to which the agent is replying. See Sections 3.7.2.3 and 3.8.3.1 for complete details.

Destination Address

Copied from the source address of the Registration Request to which the agent is replying

UDP fields:

Source Port

<variables>

Destination Port

Copied from the source port of the corresponding Registration Request (Section 3.7.1).

1627 RFC 2002 IP Mobility Support October 1996

1628

1629

1630

1631

1632

1633

1634

1635

1636

1637

1638

1639

1640

1641

1642

1643

1644

1645

1646

1647

1648

1649

1650

1651

1652

1653

1654

1655

1656

1657

1658

1659

1660

1661

1662

1663

1664

1665

1666

1667

1668

1669

1670

1671

1672

1673

1674

1675

1676

1677

1678

1679

1680

1681

1682

Perkins

Standards Track

(Page 30)

The UDP header is followed by the Mobile IP fields shown below:

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type Code Lifetime

Home Address

Home Agent

Identification

Extensions ...

Type 3 (Registration Reply)

Code A value indicating the result of the Registration Request. See below for a list of currently defined Code values.

Lifetime

If the Code field indicates that the registration was accepted, the Lifetime field is set to the number of seconds remaining before the registration is considered expired. A value of zero indicates that the mobile node has been deregistered. A value of 0xffff indicates infinity. If the Code field indicates that the registration was denied, the contents of the Lifetime field are unspecified and MUST be ignored on reception.

Home Address

The IP address of the mobile node.

Home Agent

The IP address of the mobile node's home agent.

1681 RFC 2002 IP Mobility Support October 1996

1685

1686

1687 Identification

1688 A 64-bit number used for matching Registration Requests

1689 with Registration Replies, and for protecting against

1690 replay attacks of registration messages. The value is

1691 based on the Identification field from the Registration

1692 Request message from the mobile node, and in the style of

1693 replay protection used in the security context between

1694 the mobile node and its home agent (defined by the

1695 mobility security association between them, and SPI

1696 value in the Mobile-Home Authentication Extension). See

1697 Sections 5.4 and 5.6.

1698

1699 Extensions

1700 The fixed portion of the Registration Reply is followed

1701 by one or more of the Extensions listed in Section 3.5.

1702 The Mobile-Home Authentication Extension MUST be included

1703 in all Registration Replies returned by the home agent.

1704 See Sections 3.7.2.2 and 3.8.3.3 for rules on placement

1705 of extensions to Reply messages.

1706

1707 The following values are defined for use within the Code field.

1708 Registration successful:

1709 0 registration accepted

1710 1 registration accepted, but simultaneous mobility

1711 bindings unsupported

1712

1713 Registration denied by the foreign agent:

1714 64 reason unspecified

1715 65 administratively prohibited

1716 66 insufficient resources

1717 67 mobile node failed authentication

1718 68 home agent failed authentication

1719 69 requested lifetime too long

1720 70 poorly formed Request

1721 71 poorly formed Reply

1722 72 requested encapsulation unavailable

1723 73 requested Van Jacobson compression unavailable

1724 80 home network unreachable (ICMP error received)

1725 81 home agent host unreachable (ICMP error received)

1726 82 home agent port unreachable (ICMP error received)

1727 88 home agent unreachable (other ICMP error received)

1728

1729

1730

1731

1732

1733

1734

1735

1736

1737

1738 Perkins Standards Track (Page 31)

1739 RFC 2002 IP Mobility Support October 1996

1740

1741

1742 Registration denied by the home agent:

1743 128 reason unspecified

1744 129 administratively prohibited

1745 130 insufficient resources

1746 131 mobile node failed authentication

1747 132 foreign agent failed authentication

1748 133 registration identification mismatch

1749 134 poorly formed Request

1750 135 too many simultaneous mobility bindings

1751 136 unknown home agent address

1752

1753

1754

1755 Up-to-date values of the Code field are specified in the most recent

1756 "Assigned Numbers" [20].

1757

1758 3.5. Registration Extensions

1759

1760 3.5.1. Computing Authentication Extension Values

1761

1762 The Authenticator value computed for each authentication Extension

1763 MUST protect the following fields from the registration message:

1764

1765 - the UDP payload (that is, the Registration Request or

1766 Registration Reply data),

1767

1768 - all prior Extensions in their entirety, and

1769

1770 - the Type and Length of this Extension.

1771

1772 The default authentication algorithm uses keyed-MD5 [21] in

1773 "prefix-suffix" mode to compute a 128-bit "message digest" of the

1774 registration message. The default authenticator is a 128-bit value

1775 computed as the MD5 checksum over the following stream of bytes:

1776

1777 - the shared secret defined by the mobility security association

1778 between the nodes and by SPI value specified in the

1779 authentication Extension, followed by

1780

1781 - the protected fields from the registration message, in the order

1782 specified above, followed by

1783

1784 - the shared secret again.

1785

1786 Note that the Authenticator field itself and the UDP header are NOT

1787 included in the computation of the default Authenticator value. See

1788 Section 5.1 for information about support requirements for message

1789 authentication codes, which are to be used with the various

1790 authentication Extensions.

1791

1792

1793

1794 Perkins Standards Track (Page 32)

1795 RFC 2002 IP Mobility Support October 1996

1796

1797

1798

1799

1800 The Security Parameter Index (SPI) within any of the authentication

1801 Extensions defines the security context which is used to compute the

1802 Authenticator value and which MUST be used by the receiver to check

1803 that value. In particular, the SPI selects the authentication

1804 algorithm and mode (Section 5.1) and secret (a shared key, or

1805 appropriate public/private key pair) used in computing the

1806 Authenticator. In order to ensure interoperability between different

1807 implementations of the Mobile IP protocol, an implementation MUST be

1808 able to associate any SPI value with any authentication algorithm and

1809 mode which it implements. In addition, all implementations of Mobile

1810 IP MUST implement the default authentication algorithm (keyed-MD5)

1811 and mode ("prefix-suffix") defined above.

1812

1813 5.5.2. Mobile-Home Authentication Extension

1814

1815 Exactly one Mobile-Home Authentication Extension MUST be present in

1816 all Registration Requests and Registration Replies, and is intended

1817 to eliminate problems [2] which result from the uncontrolled

1818 propagation of remote redirects in the Internet. The location of the

1819 extension marks the end of the authenticated data.

1820

1821 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

1822

1823

1824

1825

1826

1827

1828

1829

1830

1831

1832

1833

1834

1835

1836

1837

1838

1839

1840

1841

1842

1843

1844

1845

1846

1847

1848

1849

1850

Perkins

Standards Track

(Page 33)

1851 RFC 2002 IP Mobility Support October 1996

1852

1853

1854

1855

1856

1857

1858

1859

1860

1861

1862

1863

1864

1865

1866

1867

1868

1869

1870

1871

1872

1873

1874

1875

1876

1877

1878

1879

1880

1881

1882

1883

1884

1885

1886

1887

1888

1889

1890

1891

1892

1893

1894

1895

1896

1897

1898

1899

1900

1901

1902

1903

1904

1905

1906

Perkins

Standards Track

(Page 34)

1997 RFC 2002 IP Mobility Support October 1996

1998

1999

2000 For each pending registration, the mobile node maintains the following information:

2001

2002 - the link-layer address of the foreign agent to which the

2003 Registration Request was sent, if applicable,

2004 the IP destination address of the Registration Request,

2005 - the care-of address used in the registration,

2006 - the identification value sent in the registration,

2007 - the remaining requested Lifetime, and

2008 - the remaining Lifetime of the pending registration.

2009

2010 A mobile node SHOULD initiate a registration whenever it detects a

2011 change in its network connectivity. See Section 2.4.2 for methods by

2012 which mobile nodes MAY make such a determination. When it is away

2013 from home, the mobile node's registration Request allows its home

2014 agent to create or modify a mobility binding for it. When it is at

2015 home, the mobile node's (de)Registration Request allows its home

2016 agent to delete any previous mobility binding(s) for it. A mobile

2017 node operates without the support of mobility functions when it is at

2018 home.

2019

2020 There are other conditions under which the mobile node SHOULD

2021 (re)register with its foreign agent, such as when the mobile node

2022 detects that the foreign agent has rebooted (as specified in Section

2023 2.4.4) and when the current registration's Lifetime is near

2024 expiration.

2025

2026 In the absence of link-layer indications of changes in point of

2027 attachment, Agent Advertisements from new agents SHOULD NOT cause a

2028 mobile node to attempt a new registration, if its current

2029 registration has not expired and it is still also receiving Agent

2030 Advertisements from the foreign agent with which it is currently

2031 registered. In the absence of link-layer indications, a mobile node

2032 MUST NOT attempt to register more often than once per second.

2033

2034 A mobile node MAY register with a different agent when transport-

2035 layer protocols indicate excessive retransmissions. A mobile node

2036 MUST NOT consider reception of an ICMP Redirect from a foreign agent

2037 that is currently providing service to it as reason to register with

2038 a new foreign agent. Within these constraints, the mobile node MAY

2039 register again at any time.

2040

2041 Appendix D shows some examples of how the fields in registration

2042 messages would be set up in some typical registration scenarios.

2043

2044

2045

2046

2047

2048

2049

2050

2051

2052

2053

2054

2055

2056

2057

2058

2059

2060

2061

2062

Perkins

Standards Track

[Page 35]

1963 RFC 2002 IP Mobility Support October 1996

1964

1965

1966

1967 3.6.1. Sending Registration Requests

1968

1969 The following sections specify details for the values the mobile node

1970 MUST supply in the fields of Registration Request messages.

1971

1972 3.6.1.1. IP Fields

1973

1974 This section provides the specific rules by which mobile nodes pick

1975 values for the IP header fields of a Registration Request.

1976

1977 IP Source Address:

1978

1979 - When registering on a foreign network with a co-located care-of

1980 address, the IP source address MUST be the care-of address.

1981

1982 - In all other circumstances, the IP source address MUST be the

1983 mobile node's home address.

1984

1985 IP Destination Address:

1986

1987 - When the mobile node has discovered the agent with which it is

1988 registering, through some means (e.g., link-layer) that does not

1989 provide the IP address of the agent (the IP address of the agent

1990 is unknown to the mobile node), then the "All Mobility Agents"

1991 multicast address (224.0.0.11) MUST be used. In this case, the

1992 mobile node MUST use the agent's link-layer unicast address in

1993 order to deliver the datagram to the correct agent.

1994

1995 - When registering with a foreign agent, the address of the agent

1996 as learned from the IP source address of the corresponding Agent

1997 Advertisement MUST be used. In addition, when transmitting

1998 this Registration Request message, the mobile node MUST use a

1999 link-layer destination address copied from the link-layer source

2000 address of the Agent Advertisement message in which it learned

2001 this foreign agent's IP address.

2002

2003 - When the mobile node is registering directly with its home

2004 agent and knows the (unicast) IP address of its home agent, the

2005 destination address MUST be set to this address.

2006

2007

2008

2009

2010

2011

2012

2013

2014

2015

2016

2017

2018

Perkins

Standards Track

[Page 36]

May 13 1998 10:38:26			rfc2002.txt	Page 37
2019	RFC 2002	IP Mobility Support		
2020				October 1996
2021				
2022				
2023				
2024			- If the mobile node is registering directly with its home agent, but does not know the IP address of its home agent, the mobile node may use dynamic home agent address resolution to automatically determine the IP address of its home agent (Section 3.6.1.2). In this case, the IP destination address is set to the subnet-directed broadcast address of the mobile node's home network. This address MUST NOT be used as the destination IP address if the mobile node is registering via a foreign agent, although it MAY be used as the Home Agent address in the body of the Registration Request when registering via a foreign agent.	
2025			IP Time to live:	
2026				
2027			- The IP TTL field MUST be set to 1 if the IP destination address is set to the "All Mobility Agents" multicast address as described above. Otherwise a suitable value should be chosen in accordance with standard IP practice [19].	
2028				
2029				
2030				
2031				
2032				
2033				
2034				
2035				
2036				
2037				
2038				
2039				
2040				
2041			3.6.1.2. Registration Request Fields	
2042				
2043			This section provides specific rules by which mobile nodes pick values for the fields within the fixed portion of a Registration Request.	
2044				
2045				
2046				
2047			A mobile node MAY set the 'S' bit in order to request that the home agent maintain prior mobility binding(s). Otherwise, the home agent deletes any previous binding(s) and replaces them with the new binding specified in the Registration Request. Multiple simultaneous mobility bindings are likely to be useful when a mobile node using at least one wireless network interface moves within wireless transmission range of more than one foreign agent. IP explicitly allows duplication of datagrams. When the home agent allows simultaneous bindings, it will tunnel a separate copy of each arriving datagram to each care-of address, and the mobile node will receive multiple copies of datagrams destined to it.	
2048			The mobile node SHOULD set the 'D' bit if it is registering with a co-located care-of address. Otherwise, the 'D' bit MUST NOT be set.	
2049				
2050			A mobile node MAY set the 'B' bit to request its home agent to forward to it, a copy of broadcast datagrams received by its home agent from the home network. The method used by the home agent to forward broadcast datagrams depends on the type of care-of address registered by the mobile node, as determined by the 'D' bit in the mobile node's Registration Request:	
2051				
2052				
2053				
2054				
2055				
2056				
2057				
2058				
2059				
2060				
2061				
2062				
2063				
2064				
2065				
2066				
2067				
2068				
2069				
2070				
2071				
2072				
2073				
2074	Perkins	Standards Track		[Page 37]

May 13 1998 10:38:26			rfc2002.txt	Page 38
2075	RFC 2002	IP Mobility Support		October 1996
2076				
2077				
2078				
2079			- If the 'D' bit is set, then the mobile node has indicated that it will decapsulate any datagrams tunneled to this care-of address itself (the mobile node is using a co-located care-of address). In this case, to forward such a received broadcast datagram to the mobile node, the home agent MUST tunnel it to this care-of address. The mobile node de-tunnels the received datagram in the same way as any other datagram tunneled directly to it.	
2080				
2081			- If the 'D' bit is NOT set, then the mobile node has indicated that it is using a foreign agent care-of address, and that the foreign agent will thus decapsulate arriving datagrams before forwarding them to the mobile node. In this case, to forward such a received broadcast datagram to the mobile node, the home agent MUST first encapsulate the broadcast datagram in a unicast datagram addressed to the mobile node's home address, and then MUST tunnel this resulting datagram to the mobile node's care-of address.	
2082				
2083				
2084				
2085				
2086				
2087				
2088				
2089				
2090				
2091				
2092				
2093				
2094				
2095				
2096				
2097				
2098				
2099				
2100				
2101				
2102				
2103				
2104				
2105				
2106				
2107				
2108				
2109				
2110				
2111				
2112				
2113				
2114				
2115				
2116				
2117				
2118				
2119				
2120				
2121				
2122				
2123				
2124				
2125				
2126				
2127				
2128				
2129				
2130	Perkins	Standards Track		[Page 38]

2141 RFC 2002 IP Mobility Support October 1996

2142

2143 - The mobile node MAY ask a home agent to delete a particular

2144 mobility binding, by sending a Registration Request with the

2145 care-of address for this binding, with the Lifetime field set to

2146 zero (Section 3.8.2).

2147

2148 - Similarly, a Lifetime of zero is used when the mobile node

2149 deregisters all care-of addresses, such as upon returning home.

2150

2151 The Home Agent field MUST be set to the address of the mobile node's

2152 home agent, if the mobile node knows this address. Otherwise, the

2153 mobile node MAY use dynamic home agent address resolution to learn

2154 the address of its home agent. In this case, the mobile node MUST

2155 set the Home Agent field to the subnet-directed broadcast address of

2156 the mobile node's home network. Each home agent receiving such a

2157 Registration Request with a broadcast destination address MUST reject

2158 the mobile node's registration and SHOULD return a rejection

2159 Registration Reply indicating its unicast IP address for use by the

2160 mobile node in a future registration attempt.

2161

2162 The Care-of Address field MUST be set to the value of the particular

2163 care-of address that the mobile node wishes to (de)register. In the

2164 special case in which a mobile node wishes to deregister all care-of

2165 addresses, it MUST set this field to its home address.

2166

2167 The mobile node chooses the Identification field in accordance with

2168 the style of replay protection it uses with its home agent. This is

2169 part of the mobility security association the mobile node shares with

2170 its home agent. See Section 5.6 for the method by which the mobile

2171 node computes the Identification field.

2172

2173 3.6.1.3. Extensions

2174

2175 This section describes the ordering of any mandatory and any optional

2176 Extensions that a mobile node appends to a Registration Request.

2177 This following ordering MUST be followed:

2178

2179 a) The IP header, followed by the UDP header, followed by the

2180 fixed-length portion of the Registration Request, followed by

2181

2182 b) If present, any non-authentication Extensions expected to be

2183 used by the home agent (which may or may not also be used by

2184 the foreign agent), followed by

2185

2186 c) The Mobile-Home Authentication Extension, followed by

2187

2188 d) If present, any non-authentication Extensions used only by

2189 the foreign agent, followed by

2190

Perkins Standards Track [Page 39]

2187 RFC 2002 IP Mobility Support October 1996

2188

2189 e) The Mobile-Foreign Authentication Extension, if present.

2190

2191 Note that items (a) and (c) MUST appear in every Registration Request

2192 sent by the mobile node. Items (b), (d), and (e) are optional.

2193 However, item (e) MUST be included when the mobile node and the

2194 foreign agent share a mobility security association.

2195

2196 3.6.2. Receiving Registration Replies

2197

2198 Registration Replies will be received by the mobile node in response

2199 to its Registration Requests. Registration Replies generally fall

2200 into three categories:

2201

2202 - the registration was accepted,

2203 - the registration was denied by the foreign agent, or

2204 - the registration was denied by the home agent.

2205

2206 The remainder of this section describes the Registration Reply

2207 handling by a mobile node in each of these three categories.

2208

2209 3.6.2.1. Validity Checks

2210

2211 Registration Replies with an invalid, non-zero UDP checksum MUST be

2212 silently discarded.

2213

2214 In addition, the low-order 32 bits of the Identification field in the

2215 Registration Reply MUST be compared to the low-order 32 bits of the

2216 Identification field in the most recent Registration Request sent to

2217 the replying agent. If they do not match, the Reply MUST be silently

2218 discarded.

2219

2220 Also, the authentication in the Registration Reply MUST be checked.

2221 That is, the mobile node MUST check for the presence of a valid

2222 authentication Extension, acting in accordance with the Code field in

2223 the Reply. The rules are as follows:

2224

2225 a) If the mobile node and the foreign agent share a

2226 mobility security association, exactly one Mobile-Foreign

2227 Authentication Extension MUST be present in the Registration

2228 Reply, and the mobile node MUST check the Authenticator

2229 value in the Extension. If no Mobile-Foreign Authentication

2230 Extension is found, or if more than one Mobile-Foreign

2231 Authentication Extension is found, or if the Authenticator is

2232 invalid, the mobile node MUST silently discard the Reply and

2233 SHOULD log the event as a security exception.

2234

2235

2236

2237

2238

2239

2240

2241

2242 Perkins Standards Track [Page 40]

2243
2244 RFC 2002 IP Mobility Support October 1996
2245
2246
2247 b) If the Code field indicates that service is denied by
2248 the home agent, or if the Code field indicates that the
2249 registration was accepted by the home agent, exactly one
2250 Mobile-Home Authentication Extension MUST be present in
2251 the Registration Reply, and the mobile node MUST check the
2252 Authenticator value in the Extension. If no Mobile-Home
2253 Authentication Extension is found, or if more than one
2254 Mobile-Home Authentication Extension is found, or if the
2255 Authenticator is invalid, the mobile node MUST silently
2256 discard the Reply and SHOULD log the event as a security
2257 exception.
2258
2259 If the Code field indicates an authentication failure, either at the
2260 foreign agent or the home agent, then it is quite possible that any
2261 authenticators in the Registration Reply will also be in error. This
2262 could happen, for example, if the shared secret between the mobile
2263 node and home agent was erroneously configured. The mobile node
2264 SHOULD log such errors as security exceptions.
2265
2266 3.6.2.2. Registration Request Accepted
2267
2268 If the Code field indicates that the request has been accepted, the
2269 mobile node SHOULD configure its routing table appropriately for its
2270 current point of attachment (Section 4.2.1).
2271
2272 If the mobile node is returning to its home network and that network
2273 is one which implements ARP, the mobile node MUST follow the
2274 procedures described in Section 4.6 with regard to ARP, proxy ARP,
2275 and gratuitous ARP.
2276
2277 If the mobile node has registered on a foreign network, it SHOULD
2278 re-register before the expiration of the Lifetime of its
2279 registration. As described in Section 3.6, for each pending
2280 Registration Request, the mobile node MUST maintain the remaining
2281 lifetime of this pending registration, as well as the original
2282 lifetime from the Registration Request. When the mobile node
2283 receives a valid Registration Reply, the mobile node MUST decrease
2284 its view of the remaining lifetime of the registration by the amount
2285 by which the home agent decreased the originally requested Lifetime.
2286 This procedure is equivalent to the mobile node starting a timer for
2287 the granted Lifetime at the time it sent the Registration Request,
2288 even though the granted Lifetime is not known to the mobile node
2289 until the Registration Reply is received. Since the Registration
2290 Request is certainly sent before the home agent begins timing the
2291 registration Lifetime (also based on the granted Lifetime), this
2292 procedure ensures that the mobile node will re-register before the
2293 home agent expires and deletes the registration, in spite of possibly
2294 non-negligible transmission delays for the original Registration
2295
2296
2297
2298 Perkins Standards Track (Page 41)

2299 RFC 2002 IP Mobility Support October 1996
2300
2301
2302 Request and Reply that started the timing of the Lifetime at the
2303 mobile node and its home agent.
2304
2305 3.6.2.3. Registration Request Denied
2306
2307 If the Code field indicates that service is being denied, the mobile
2308 node SHOULD log the error. In certain cases the mobile node may be
2309 able to "repair" the error. These include:
2310
2311 Code 69: (Denied by foreign agent, Lifetime too long)
2312
2313 In this case, the Lifetime field in the Registration Reply will
2314 contain the maximum Lifetime value which that foreign agent is
2315 willing to accept in any Registration Request. The mobile node
2316 MAY attempt to register with this same agent, using a Lifetime
2317 in the Registration Request that MUST be less than or equal to
2318 the value specified in the Reply.
2319
2320 Code 133: (Denied by home agent, Identification mismatch)
2321
2322 In this case, the Identification field in the Registration
2323 Reply will contain a value that allows the mobile node to
2324 synchronize with the home agent, based upon the style of replay
2325 protection in effect (Section 5.6). The mobile node MUST
2326 adjust the parameters it uses to compute the Identification
2327 field based upon the information in the Registration Reply,
2328 before issuing any future Registration Requests.
2329
2330 Code 136: (Denied by home agent, Unknown home agent address)
2331
2332 This code is returned by a home agent when the mobile node is
2333 performing dynamic home agent address resolution as described
2334 in Sections 3.6.1.1 and 3.6.1.2. In this case, the Home Agent
2335 field within the Reply will contain the unicast IP address of
2336 the home agent returning the Reply. The mobile node MAY then
2337 attempt to register with this home agent in future Registration
2338 Requests. In addition, the mobile node SHOULD adjust the
2339 parameters it uses to compute the Identification field based
2340 upon the corresponding field in the Registration Reply, before
2341 issuing any future Registration Requests.
2342
2343 3.6.3. Registration Retransmission
2344
2345 When no Registration Reply has been received within a reasonable
2346 time, another Registration Request MAY be transmitted. When
2347 timestamps are used, a new Registration Identification is chosen for
2348 each retransmission; thus it counts as a new registration. When
2349 nonces are used, the unanswered Request is retransmitted unchanged;
2350
2351
2352
2353
2354 Perkins Standards Track (Page 42)

2355 RFC 2002 IP Mobility Support October 1996

2356

2357

2358

2359 thus the retransmission does not count as a new registration (Section

2360 5.6). In this way a retransmission will not require the home agent

2361 to resynchronize with the mobile node by issuing another nonce in the

2362 case in which the original Registration Request (rather than its

2363 Registration Reply) was lost by the network.

2364

2365 The maximum time until a new Registration Request is sent SHOULD be

2366 no greater than the requested Lifetime of the Registration Request.

2367 The minimum value SHOULD be large enough to account for the size of

2368 the messages, twice the round trip time for transmission to the home

2369 agent, and at least an additional 100 milliseconds to allow for

2370 processing the messages before responding. The round trip time for

2371 transmission to the home agent will be at least as large as the time

2372 required to transmit the messages at the link speed of the mobile

2373 node's current point of attachment. Some circuits add another 200

2374 milliseconds of satellite delay in the total round trip time to the

2375 home agent. The minimum time between Registration Requests MUST NOT

2376 be less than 1 second. Each successive retransmission timeout period

2377 SHOULD be at least twice the previous period, as long as that is less

2378 than the maximum as specified above.

2379

2380 3.7. Foreign Agent Considerations

2381

2382 The foreign agent plays a mostly passive role in Mobile IP

2383 registration. It relays Registration Requests between mobile nodes

2384 and home agents, and, when it provides the care-of address,

2385 decapsulates datagrams for delivery to the mobile node. It SHOULD

2386 also send periodic Agent Advertisement messages to advertise its

2387 presence as described in Section 2.3, if not detectable by link-layer

2388 means.

2389

2390 A foreign agent MUST NOT transmit a Registration Request except when

2391 relaying a Registration Request received from a mobile node, to the

2392 mobile node's home agent. A foreign agent MUST NOT transmit a

2393 Registration Reply except when relaying a Registration Reply received

2394 from a mobile node's home agent, or when replying to a Registration

2395 Request received from a mobile node in the case in which the foreign

2396 agent is denying service to the mobile node. In particular, a

2397 foreign agent MUST NOT generate a Registration Request or Reply

2398 because a mobile node's registration Lifetime has expired. A foreign

2399 agent also MUST NOT originate a Registration Request message that

2400 asks for deregistration of a mobile node; however, it MUST relay

2401 valid (de)Registration Requests originated by a mobile node.

2402

2403

2404

2405

2406

2407

2408

2409

2410 Perkins Standards Track [Page 43]

2411 RFC 2002 IP Mobility Support October 1996

2412

2413

2414

2415 3.7.1. Configuration and Registration Tables

2416

2417 Each foreign agent MUST be configured with a care-of address. In

2418 addition, for each pending or current registration, the foreign agent

2419 MUST maintain a visitor list entry containing the following

2420 information obtained from the mobile node's Registration Request:

2421

2422 - the link-layer source address of the mobile node

2423 - the IP Source Address (the mobile node's Home Address)

2424 - the IP Destination Address (as specified in 3.6.2.3)

2425 - the UDP Source Port

2426 - the Home Agent address

2427 - the Identification field

2428 - the requested registration Lifetime, and

2429 - the remaining Lifetime of the pending or current registration.

2430

2431 As with any node on the Internet, a foreign agent MAY also share

2432 mobility security associations with any other nodes. When relaying a

2433 Registration Request from a mobile node to its home agent, if the

2434 foreign agent shares a mobility security association with the home

2435 agent, it MUST add a Foreign-Home Authentication Extension to the

2436 Request and MUST check the required Foreign-Home Authentication

2437 Extension in the Registration Reply from the home agent (Sections 3.3

2438 and 3.4). Similarly, when receiving a Registration Request from a

2439 mobile node, if the foreign agent shares a mobility security

2440 association with the mobile node, it MUST check the required Mobile-

2441 Foreign Authentication Extension in the Request and MUST add a

2442 Mobile-Foreign Authentication Extension to the Registration Reply to

2443 the mobile node.

2444

2445 3.7.2. Receiving Registration Requests

2446

2447 If the foreign agent accepts a Registration Request from a mobile

2448 node, it then MUST relay the Request to the indicated home agent.

2449 Otherwise, if the foreign agent denies the Request, it MUST send a

2450 Registration Reply to the mobile node with an appropriate denial

2451 Code, except in cases where the foreign agent would be required to

2452 send out more than one such denial per second to the same mobile

2453 node. The following sections describe this behavior in more detail.

2454

2455 If a foreign agent receives a Registration Request from a mobile node

2456 in its visitor list, the existing visitor list entry for the mobile

2457 node SHOULD NOT be deleted or modified until the foreign agent

2458 receives a valid Registration Reply from the home agent with a Code

2459 indicating success. The foreign agent MUST record the new pending

2460

2461

2462

2463

2464

2465

2466 Perkins Standards Track [Page 44]

2467 RFC 2002 IP Mobility Support October 1996

2468

2469

2470

2471 Request separately from the existing visitor list entry for the

2472 mobile node. If the Registration Request requests deregistration,

2473 the existing visitor list entry for the mobile node SHOULD NOT be

2474 deleted until the foreign agent has received a successful

2475 Registration Reply. If the Registration Reply indicates that the

2476 Request (for registration or deregistration) was denied by the home

2477 agent, the existing visitor list entry for the mobile node MUST NOT

2478 be modified as a result of receiving the Registration Reply.

2479

2480 3.7.2.1. Validity Checks

2481

2482 Registration Requests with an invalid, non-zero UDP checksum MUST be

2483 silently discarded.

2484

2485 Also, the authentication in the Registration Request MUST be checked.

2486 If the foreign agent and the mobile node share a mobility security

2487 association, exactly one Mobile-Foreign Authentication Extension MUST

2488 be present in the Registration Request, and the foreign agent MUST

2489 check the Authenticator value in the Extension. If no Mobile-Foreign

2490 Authentication Extension is found, or if more than one Mobile-Foreign

2491 Authentication Extension is found, or if the Authenticator is

2492 invalid, the foreign agent MUST silently discard the Request and

2493 SHOULD log the event as a security exception. The foreign agent also

2494 SHOULD send a Registration Reply to the mobile node with Code 67.

2495

2496 3.7.2.2. Forwarding a Valid Request to the Home Agent

2497

2498 If the foreign agent accepts the mobile node's Registration Request,

2499 it MUST relay the Request to the mobile node's home agent as

2500 specified in the Home Agent field of the Registration Request. The

2501 foreign agent MUST NOT modify any of the fields beginning with the

2502 fixed portion of the Registration Request up through and including

2503 the Mobile-Home Authentication Extension. Otherwise, an

2504 authentication failure is very likely to occur at the home agent. In

2505 addition, the foreign agent proceeds as follows:

2506

- It MUST process and remove any Extensions following the
- Mobile-Home Authentication Extension.
- It MAY append any of its own non-authentication Extensions of
- relevance to the home agent, if applicable, and
- It MUST append the Foreign-Home Authentication Extension, if the

2513 foreign agent shares a mobility security association with the home

2514 agent.

2515

2516

2517

2518

2519

2520

2521 Perkins

2522 Standards Track (Page 45)

2523 RFC 2002 IP Mobility Support October 1996

2524

2525

2526

2527 Specific fields within the IP header and the UDP header of the

2528 relayed Registration Request MUST be set as follows:

2529

2530 IP Source Address

2531 The foreign agent's address on the interface from which

2532 the message will be sent.

2533

2534 IP Destination Address

2535 Copied from the Home Agent field within the Registration

2536 Request.

2537

2538 UDP Source Port

2539 <variable>

2540

2541 UDP Destination Port

2542 434

2543

2544 After forwarding a valid Registration Request to the home agent, the

2545 foreign agent MUST begin timing the remaining lifetime of the pending

2546 registration based on the Lifetime in the Registration Request. If

2547 this lifetime expires before receiving a valid Registration Reply, the

2548 foreign agent MUST delete its visitor list entry for this pending

2549 registration.

2550

2551 3.7.2.3. Denying Invalid Requests

2552

2553 If the foreign agent denies the mobile node's Registration Request

2554 for any reason, it SHOULD send the mobile node a Registration Reply

2555 with a suitable denial Code. In such a case, the Home Address, Home

2556 Agent, and Identification fields within the Registration Reply are

2557 copied from the corresponding fields of the Registration Request.

2558

2559 If the Reserved field is nonzero, the foreign agent MUST deny the

2560 Request and SHOULD return a Registration Reply with status code 70 to

2561 the mobile node. If the Request is being denied because the

2562 requested Lifetime is too long, the foreign agent sets the Lifetime

2563 in the Reply to the maximum Lifetime value it is willing to accept in

2564 any Registration Request, and sets the Code field to 69. Otherwise,

2565 the Lifetime SHOULD be copied from the Lifetime field in the Request.

2566

2567 Specific fields within the IP header and the UDP header of the

2568 Registration Reply MUST be set as follows:

2569

2570 IP Source Address

2571 Copied from the IP Destination Address of Registration

2572 Request, unless the "All Agents Multicast" address was

2573 used. In this case, the foreign agent's address (on the

2574 interface from which the message will be sent) MUST be

2575

2576

2577 Perkins

2578 Standards Track (Page 46)

May 13 1998 10:38:26		rfc2002.txt	Page 47
2579	RFC: 2002	IP Mobility Support	October 1996
2580			
2581			
2582		used.	
2583			
2584			
2585		IP Destination Address	
2586		Copied from the IP Source Address of the Registration	
2587		Request.	
2588			
2589		UDP Source Port	
2590		434	
2591			
2592		UDP Destination Port	
2593		Copied from the UDP Source Port of the Registration	
2594		Request.	
2595			
2596		3.7.3. Receiving Registration Replies	
2597			
2598		The foreign agent updates its visitor list when it receives a valid	
2599		Registration Reply from a home agent. It then relays the	
2600		Registration Reply to the mobile node. The following sections	
2601		describe this behavior in more detail.	
2602			
2603		If upon relaying a Registration Request to a home agent, the foreign	
2604		agent receives an ICMP error message instead of a Registration Reply,	
2605		then the foreign agent SHOULD send to the mobile node a Registration	
2606		Reply with an appropriate "Home Agent Unreachable" failure Code	
2607		(within the range 80-95, inclusive). See Section 3.7.2.3 for details	
2608		on building the Registration Reply.	
2609			
2610		3.7.3.1. Validity Checks	
2611			
2612		Registration Replies with an invalid, non-zero UDP checksum MUST be	
2613		silently discarded.	
2614			
2615		When a foreign agent receives a Registration Reply message, it MUST	
2616		search its visitor list for a pending Registration Request with the	
2617		same mobile node home address as indicated in the Reply. If no	
2618		pending Request is found, the foreign agent MUST silently discard the	
2619		Reply. The foreign agent MUST also silently discard the Reply if the	
2620		low-order 32 bits of the Identification field in the Reply do not	
2621		match those in the Request.	
2622			
2623		Also, the authentication in the Registration Reply MUST be checked.	
2624		If the foreign agent and the home agent share a mobility security	
2625		association, exactly one Foreign-Home Authentication Extension MUST	
2626		be present in the Registration Reply, and the foreign agent MUST	
2627		check the Authenticator value in the Extension. If no Foreign-Home	
2628		Authentication Extension is found, or if more than one Foreign-Home	
2629		Authentication Extension is found, or if the Authenticator is	
2630		invalid, the foreign agent MUST silently discard the Reply and SHOULD	
2631			
2632			
2633	Perkins	Standards Track	(Page 47)
2634			

May 13 1998 10:38:26		rfc2002.txt	Page 48
2635	RFC: 2002	IP Mobility Support	October 1996
2636			
2637			
2638			
2639		log the event as a security exception. The foreign agent also MUST	
2640		reject the mobile node's registration and SHOULD send a Registration	
2641		Reply to the mobile node with Code 68.	
2642			
2643		3.7.3.2. Forwarding Replies to the Mobile Node	
2644			
2645		A Registration Reply which satisfies the validity checks of Section	
2646		3.8.2.1 is relayed to the mobile node. The foreign agent MUST also	
2647		update its visitor list entry for the mobile node to reflect the	
2648		results of the Registration Request, as indicated by the Code field	
2649		in the Reply. If the Code indicates that the mobile node has	
2650		accepted the registration and the Lifetime field is nonzero, the	
2651		foreign agent MUST set the Lifetime in the visitor list entry to the	
2652		value specified in the Lifetime field of the Registration Reply. If,	
2653		instead, the Code indicates that the Lifetime field is zero, the	
2654		foreign agent MUST delete its visitor list entry for the mobile node.	
2655		Finally, if the Code indicates that the registration was denied by	
2656		the home agent, the foreign agent MUST delete its pending	
2657		registration list entry, but not its visitor list entry, for the	
2658		mobile node.	
2659			
2660		The foreign agent MUST NOT modify any of the fields beginning with	
2661		the fixed portion of the Registration Reply up through and including	
2662		the Mobile-Home Authentication Extension. Otherwise, an	
2663		authentication failure is very likely to occur at the mobile node.	
2664		In addition, the foreign agent SHOULD perform the following	
2665		additional procedures:	
2666			
2667		- It MUST process and remove any Extensions following the	
2668		Mobile-Home Authentication Extension,	
2669		- It MAY append its own non-authentication Extensions of relevance	
2670		to the mobile node, if applicable, and	
2671		- It MUST append the Mobile-Foreign Authentication Extension, if	
2672		the foreign agent shares a mobility security association with the	
2673		mobile node.	
2674			
2675		Specific fields within the IP header and the UDP header of the	
2676		relayed Registration Reply are set according to the same rules	
2677		specified in Section 3.7.2.3.	
2678			
2679		After forwarding a valid Registration Reply to the mobile node, the	
2680		foreign agent MUST update its visitor list entry for this	
2681		registration as follows. If the Registration Reply indicates that	
2682		the registration was accepted by the home agent, the foreign agent	
2683		resets its timer of the lifetime of the registration to the lifetime	
2684		granted in the Registration Reply; unlike the mobile node's timing of	
2685		the registration lifetime as described in Section 3.6.2.2, the	
2686		foreign agent considers this lifetime to begin when it forwards the	
2687			
2688			
2689			
2690	Perkins	Standards Track	(Page 48)

2691
2692
2693
2694
2695
2696
2697
2698
2699
2700
2701
2702
2703
2704
2705
2706
2707
2708
2709
2710
2711
2712
2713
2714
2715
2716
2717
2718
2719
2720
2721
2722
2723
2724
2725
2726
2727
2728
2729
2730
2731
2732
2733
2734
2735
2736
2737
2738
2739
2740
2741
2742
2743
2744
2745
2746

RFC 2002

IP Mobility Support

October 1996

Registration Reply message, ensuring that the foreign agent will not expire the registration before the mobile node does. On the other hand, if the Registration Reply indicates that the registration was rejected by the home agent, the foreign agent deletes its visitor list entry for this attempted registration.

3.8. Home Agent Considerations

Home agents play a reactive role in the registration process. The home agent receives Registration Requests from the mobile node (perhaps relayed by a foreign agent), updates its record of the mobility bindings for this mobile node, and issues a suitable Registration Reply in response to each.

A home agent MUST NOT transmit a Registration Reply except when replying to a Registration Request received from a mobile node. In particular, the home agent MUST NOT generate a Registration Reply to indicate that the Lifetime has expired.

3.8.1. Configuration and Registration Tables

Each home agent MUST be configured with an IP address and with the prefix size for the home network. The home agent MUST be configured with the home address and mobility security association of each authorized mobile node that it is serving as a home agent. When the home agent accepts a valid Registration Request from a mobile node that it serves as a home agent, the home agent MUST create or modify the entry for this mobile node in its mobility binding list containing:

- the mobile node's care-of address
- the Identification field from the Registration Reply
- the remaining Lifetime of the registration

The home agent MAY also maintain mobility security associations with various foreign agents. When receiving a Registration Request from a foreign agent, if the home agent shares a mobility security association with the foreign agent, the home agent MUST check the Authenticator in the required Foreign-Home Authentication Extension in the message, based on this mobility security association. Similarly, when sending a Registration Reply to a foreign agent, if the home agent shares a mobility security association with the foreign agent, the home agent MUST include a Foreign-Home Authentication Extension in the message, based on this mobility security association.

3.8.2. Receiving Registration Requests

Perkins

Standards Track

(Page 49)

2747
2748
2749
2750
2751
2752
2753
2754
2755
2756
2757
2758
2759
2760
2761
2762
2763
2764
2765
2766
2767
2768
2769
2770
2771
2772
2773
2774
2775
2776
2777
2778
2779
2780
2781
2782
2783
2784
2785
2786
2787
2788
2789
2790
2791
2792
2793
2794
2795
2796
2797
2798
2799
2800
2801
2802

RFC 2002

IP Mobility Support

October 1996

If the home agent accepts an incoming Registration Request, it MUST update its record of the mobile node's mobility binding(s) and SHOULD send a Registration Reply with a suitable Code. Otherwise (the home agent denies the Request), it SHOULD send a Registration Reply with an appropriate Code specifying the reason the Request was denied. The following sections describe this behavior in more detail.

3.8.2.1. Validity Checks

Registration Requests with an invalid, non-zero UDP checksum MUST be silently discarded by the home agent.

The authentication in the Registration Request MUST be checked. This involves the following operations:

- a) The home agent MUST check for the presence of a valid Mobile-Home Authentication Extension, and perform the indicated authentication. Exactly one Mobile-Home Authentication Extension MUST be present in the Registration Request, and the home agent MUST check the Authenticator value in the Extension. If no Mobile-Home Authentication Extension is found, or if more than one Mobile-Home Authentication Extension is found, or if the Authenticator is invalid, the home agent MUST reject the mobile node's registration and SHOULD send a Registration Reply to the mobile node with Code 131. The home agent MUST then discard the Request and SHOULD log the error as a security exception.
- b) The home agent MUST check that the registration Identification field is correct using the context selected by the SPI within the Mobile-Home Authentication Extension. See Section 5.6 for a description of how this is performed. If incorrect, the home agent MUST reject the Request and SHOULD send a Registration Reply to the mobile node with Code 133, including an Identification field computed in accordance with the rules specified in Section 5.6. The home agent MUST do no further processing with such a Request, though it SHOULD log the error as a security exception.
- c) If the home agent shares a mobility security association with the foreign agent, the home agent MUST check for the presence of a valid Foreign-Home Authentication Extension. Exactly one Foreign-Home Authentication Extension MUST be present in the Registration Request in this case, and the home agent MUST check the Authenticator value in the Extension. If no Foreign-Home Authentication Extension is found, or if more than one Foreign-Home Authentication Extension is found, or

Perkins

Standards Track

(Page 50)

May 13 1998 10:38:26		rfc2002.txt	Page 51
2803 2804 2805 2806 2807 2808 2809 2810 2811 2812 2813 2814 2815 2816 2817 2818 2819 2820 2821 2822 2823 2824 2825 2826 2827 2828 2829 2830 2831 2832 2833 2834 2835 2836 2837 2838 2839 2840 2841 2842 2843 2844 2845 2846 2847 2848 2849 2850 2851 2852 2853 2854 2855 2856 2857 2858	RFC 2002	IP Mobility Support	October 1996
<p>if the Authenticator is invalid, the home agent MUST reject the mobile node's registration and SHOULD send a Registration Reply to the mobile node with Code 132. The home agent MUST then discard the Request and SHOULD log the error as a security exception.</p> <p>In addition to checking the authentication in the Registration Request, home agents MUST deny Registration Requests that are sent to the subnet-directed broadcast address of the home network (as opposed to being unicast to the home agent). The home agent MUST discard the Request and SHOULD return a Registration Reply with a Code of 136. In this case, the Registration Reply will contain the home agent's unicast address, so that the mobile node can re-issue the Registration Request with the correct home agent address.</p> <p>3.8.2.2. Accepting a Valid Request</p> <p>If the Registration Request satisfies the validity checks in Section 3.8.2.1, and the home agent is able to accommodate the Request, the home agent MUST update its mobility binding list for the requesting mobile node and MUST return a Registration Reply to the mobile node. In this case, the Reply Code will be either 0 if the home agent supports simultaneous mobility bindings, or 1 if it does not. See Section 3.8.3 for details on building the Registration Reply message.</p> <p>The home agent updates its record of the mobile node's mobility bindings as follows, based on the fields in the Registration Request:</p> <ul style="list-style-type: none"> - If the Lifetime is zero and the Care-of Address equals the mobile node's home address, the home agent deletes all of the entries in the mobility binding list for the requesting mobile node. This is how a mobile node requests that its home agent cease providing mobility services. - If the Lifetime is zero and the Care-of Address does not equal the mobile node's home address, the home agent deletes only the entry containing the specified Care-of Address from the mobility binding list for the requesting mobile node. Any other active entries containing other care-of addresses will remain active. - If the Lifetime is nonzero, the home agent adds an entry containing the requested Care-of Address to the mobility binding list for the mobile node. If the 'S' bit is set and the home agent supports simultaneous mobility bindings, the previous mobility binding entries are retained. Otherwise, the home agent removes all previous entries in the mobility binding list for the mobile node. 			
Perkins			Standards Track
			[Page 51]

May 13 1998 10:38:26		rfc2002.txt	Page 52
2859 2860 2861 2862 2863 2864 2865 2866 2867 2868 2869 2870 2871 2872 2873 2874 2875 2876 2877 2878 2879 2880 2881 2882 2883 2884 2885 2886 2887 2888 2889 2890 2891 2892 2893 2894 2895 2896 2897 2898 2899 2900 2901 2902 2903 2904 2905 2906 2907 2908 2909 2910 2911 2912 2913 2914	RFC 2002	IP Mobility Support	October 1996
<p>In all cases, the home agent MUST send a Registration Reply to the source of the Registration Request, which might indeed be a different foreign agent than that whose care-of address is being (de)registered. If the home agent shares a mobility security association with the foreign agent whose care-of address is being deregistered, and that foreign agent is different from the one which relayed the Registration Request, the home agent MAY additionally send a Registration Reply to the foreign agent whose care-of address is being deregistered. The home agent MUST NOT send such a Reply if it does not share a mobility security association with the foreign agent. If no Reply is sent, the foreign agent's visitor list will expire naturally when the original Lifetime expires.</p> <p>The home agent MUST NOT increase the Lifetime above that specified by the mobile node in the Registration Request. However, it is not an error for the mobile node to request a Lifetime longer than the home agent is willing to accept. In this case, the home agent simply reduces the Lifetime to a permissible value and returns this value in the Registration Reply. The Lifetime value and returns this value in the Registration Reply. The Lifetime value in the Registration Reply informs the mobile node of the granted lifetime of the registration, indicating when it SHOULD re-register in order to maintain continued service. After the expiration of this registration lifetime, the home agent MUST delete its entry for this registration in its mobility binding list.</p> <p>If the Registration Request duplicates an accepted current Registration Request, the new Lifetime MUST NOT extend beyond the Lifetime originally granted. A Registration Request is a duplicate if the home address, care-of address, and identification fields all equal those of an accepted current registration.</p> <p>In addition, if the home network implements ARP [16], and the Registration Request asks the home agent to create a mobility binding for a mobile node which previously had no binding (the mobile node was previously assumed to be at home), then the home agent MUST follow the procedures described in Section 4.6 with regard to ARP, proxy ARP, and gratuitous ARP. If the mobile node already had a previous mobility binding, the home agent MUST continue to follow the rules for proxy ARP described in Section 4.6.</p> <p>3.8.2.3. Denying an Invalid Request</p> <p>If the Registration Reply does not satisfy all of the validity checks in Section 3.8.2.1, or the home agent is unable to accommodate the Request, the home agent SHOULD return a Registration Reply to the mobile node with a Code that indicates the reason for the error. If a foreign agent was involved in relaying the Request, this allows the foreign agent to delete its pending visitor list entry. Also, this</p>			
Perkins			Standards Track
			[Page 52]

2915 RFC 2002 IP Mobility Support October 1996

2916

2917 informs the mobile node of the reason for the error such that it may

2918 attempt to fix the error and issue another Request.

2919

2920 This section lists a number of reasons the home agent might reject a

2921 Request, and provides the Code value it should use in each instance.

2922 See Section 3.8.3 for additional details on building the Registration

2923 Reply message.

2924

2925 Many reasons for rejecting a registration are administrative in

2926 nature. For example, a home agent can limit the number of

2927 simultaneous registrations for a mobile node, by rejecting any

2928 registrations that would cause its limit to be exceeded, and

2929 returning a Registration Reply with error code 135. Similarly, a

2930 home agent may refuse to grant service to mobile nodes which have

2931 entered unauthorized service areas by returning a Registration Reply

2932 with a Code of 129.

2933

2934 If the Reserved field is nonzero, it MUST deny the Request with a

2935 Code of 134.

2936

2937 3.8.3. Sending Registration Replies

2938

2939 If the home agent accepts a Registration Request, it then MUST update

2940 its record of the mobile node's mobility binding(s) and SHOULD send a

2941 Registration Reply with a suitable Code. Otherwise (the home agent

2942 has denied the Request), it SHOULD send a Registration Reply with an

2943 appropriate Code specifying the reason the Request was denied. The

2944 following sections provide additional detail for the values the home

2945 agent MUST supply in the fields of Registration Reply messages.

2946

2947 3.8.3.1. IP/UDP Fields

2948

2949 This section provides the specific rules by which mobile nodes pick

2950 values for the IP and UDP header fields of a Registration Reply.

2951

2952 IP Source Address

2953 Copied from the IP Destination Address of Registration

2954 Request, unless a multicast or broadcast address was

2955 used. If the IP Destination Address of the Registration

2956 Request was a broadcast or multicast address, the IP

2957 Source Address of the Registration Reply MUST be set to

2958 the home agent's (unicast) IP address.

2959

2960 IP Destination Address

2961 Copied from the IP Source Address of the Registration

2962 Request.

2963

2964 Standards Track

2965

2966

2967

2968

2969

2970 Perkins [Page 53]

2971 RFC 2002 IP Mobility Support October 1996

2972

2973 UDP Source Port

2974 Copied from the UDP Destination Port of the Registration

2975 Request.

2976

2977 UDP Destination Port

2978 Copied from the UDP Source Port of the Registration

2979 Request.

2980

2981 When sending a Registration Reply in response to a Registration

2982 Request that requested deregistration of the mobile node (the

2983 Lifetime is zero and the Care-of Address equals the mobile node's

2984 home address) and in which the IP Source Address was also set to the

2985 mobile node's home address (this is the normal method used by a

2986 mobile node to deregister when it returns to its home network), the

2987 IP Destination Address in the Registration Reply will be set to the

2988 mobile node's home address, as copied from the IP Source Address of

2989 the Request.

2990

2991 In this case, when transmitting the Registration Reply, the home

2992 agent MUST transmit the Reply directly onto the home network as if

2993 the mobile node were at home, bypassing any mobility binding list

2994 entry that may still exist at the home agent for the destination

2995 mobile node. In particular, for a mobile node returning home after

2996 being registered with a care-of address, if the mobile node's new

2997 Registration Request is not accepted by the home agent, the mobility

2998 binding list entry for the mobile node will still indicate that

2999 datagrams addressed to the mobile node should be tunneled to the

3000 mobile node's registered care-of address; when sending the

3001 Registration Reply indicating the rejection of this Request, this

3002 existing binding list entry MUST be ignored, and the home agent MUST

3003 transmit this Reply as if the mobile node were at home.

3004

3005 3.8.3.2. Registration Reply Fields

3006

3007 This section provides specific rules by which home agents pick values

3008 for the fields within the fixed portion of a Registration Reply. The

3009 Code field of the Registration Reply is chosen in accordance with the

3010 rules specified in the previous sections. When replying to an

3011 accepted registration, a home agent SHOULD respond with Code 1 if it

3012 does not support simultaneous registrations.

3013

3014 The Lifetime field MUST be copied from the corresponding field in the

3015 Registration Request, unless the requested value is greater than the

3016 maximum length of time the home agent is willing to provide the

3017 requested service. In such a case, the Lifetime MUST be set to the

3018 length of time that service will actually be provided by the home

3019 agent. This reduced Lifetime SHOULD be the maximum Lifetime allowed

3020 by the home agent (for this mobile node and care-of address).

3021

3022

3023

3024

3025

3026 Standards Track

3027

3028

3029

3030

3031

3032

3033

3034

3035

3036 Perkins [Page 54]

3028 RFC 2002 IP Mobility Support October 1996

3029

3030 The Home Address field MUST be copied from the corresponding field in

3031 the Registration Request.

3032

3033 If the Home Agent field in the Registration Request contains a

3034 unicast address of this home agent, then that field MUST be copied

3035 into the Home Agent field of the Registration Reply. Otherwise, the

3036 home agent MUST set the Home Agent field in the Registration Reply to

3037 its unicast address. In this latter case, the home agent MUST reject

3038 the registration with a suitable code (e.g., Code 136) to prevent the

3039 mobile node from possibly being simultaneously registered with two or

3040 more home agents.

3041

3042 3.8.3.3. Extensions

3043

3044 This section describes the ordering of any required and any optional

3045 Mobile IP Extensions that a home agent appends to a Registration

3046 Reply. The following ordering MUST be followed:

3047

3048 a) The IP header, followed by the UDP header, followed by the

3049 fixed-length portion of the Registration Reply.

3050

3051 b) If present, any non-authentication Extensions used by the

3052 mobile node (which may or may not also be used by the foreign

3053 agent).

3054

3055 c) The Mobile-Home Authentication Extension.

3056

3057 d) If present, any non-authentication Extensions used only by

3058 the foreign agent, and

3059

3060 e) The Foreign-Home Authentication Extension, if present.

3061

3062 Note that items (a) and (c) MUST appear in every Registration Reply

3063 sent by the home agent. Items (b), (d), and (e) are optional.

3064 However, item (e) MUST be included when the home agent and the

3065 foreign agent share a mobility security association.

3066

3067 4. Routing Considerations

3068

3069 This section describes how mobile nodes, home agents, and (possibly)

3070 foreign agents cooperate to route datagrams to/from mobile nodes that

3071 are connected to a foreign network. The mobile node informs its home

3072 agent of its current location using the registration procedure

3073 described in Section 3. See the protocol overview in Section 1.7 for

3074 the relative locations of the mobile node's home address with respect

3075 to its home agent, and the mobile node itself with respect to any

3076 foreign agent with which it might attempt to register.

3077

3078

3079

3080

3081

3082

Perkins

Standards Track

(Page 55)

3083 RFC 2002 IP Mobility Support October 1996

3084

3085 4.1. Encapsulation Types

3086

3087 Home agents and foreign agents MUST support tunneling datagrams using

3088 IP in IP encapsulation [14]. Any mobile node that uses a co-located

3089 care-of address MUST support receiving datagrams tunneled using IP in

3090 IP encapsulation. Minimal encapsulation [15] and GRE encapsulation

3091 [18] are alternate encapsulation methods which MAY optionally be

3092 supported by mobility agents and mobile nodes. The use of these

3093 alternative forms of encapsulation, when requested by the mobile

3094 node, is otherwise at the discretion of the home agent.

3095

3096 4.2. Unicast Datagram Routing

3097

3098 4.2.1. Mobile Node Considerations

3099

3100 When connected to its home network, a mobile node operates without

3101 the support of mobility services. That is, it operates in the same

3102 way as any other (fixed) host or router. The method by which a

3103 mobile node selects a default router when connected to its home

3104 network, or when away from home and using a co-located care-of

3105 address, is outside the scope of this document. ICMP Router

3106 Advertisement [4] is one such method.

3107

3108 When registered on a foreign network, the mobile node chooses a

3109 default router by the following rules:

3110

3111 - If the mobile node is registered using a foreign agent care-of

3112 address, then the mobile node MUST choose its default router

3113 from among the Router Addresses advertised in the ICMP Router

3114 Advertisement portion of that Agent Advertisement message. The

3115 mobile node MAY also consider the IP source address of the Agent

3116 Advertisement as another possible choice for the IP address of a

3117 default router, along with the (possibly empty) list of Router

3118 Addresses from the ICMP Router Advertisement portion of the

3119 message. In such cases, the IP source address MUST be considered

3120 to be the worst choice (lowest preference) for a default router.

3121

3122 - If the mobile node is registered directly with its home agent

3123 using a co-located care-of address, then the mobile node SHOULD

3124 choose its default router from among those advertised in any

3125 ICMP Router Advertisement message that it receives for which

3126 its externally obtained care-of address and the Router Address

3127 match under the network prefix. If the mobile node's externally

3128 obtained care-of address matches the IP source address of the

3129 Agent Advertisement under the network prefix, the mobile node

3130 MAY also consider that IP source address as another possible

3131 choice for the IP address of a default router, along with the

3132 (possibly empty) list of Router Addresses from the ICMP Router

3133

3134

3135

3136

3137

3138

Perkins

Standards Track

(Page 56)

May 13 1998 10:38:26		rfc2002.txt	Page 57
3139	RFC 2002	IP Mobility Support	October 1996
3140	Advertisement portion of the message. If so, the IP source		
3141	address MUST be considered to be the worst choice (lowest		
3142	preference) for a default router. The network prefix MAY		
3143	be obtained from the Prefix-Lengths Extension in the Router		
3144	Advertisement, if present. The prefix MAY also be obtained		
3145	through other mechanisms beyond the scope of this document.		
3146	Beyond these rules, the actual selection of the default router is		
3147	made by the selection method specified for ICMP Router Discovery		
3148	among the Router Addresses specified above. In any case, a mobile		
3149	node registered via a foreign agent MAY choose its foreign agent as a		
3150	default router.		
3151	Note that Van Jacobson header compression [10] will not function		
3152	properly unless all TCP IP datagrams to and from the mobile node		
3153	pass, respectively, through the same first and last-hop router. The		
3154	mobile node, therefore, MUST select its foreign agent as its default		
3155	router if it performs Van Jacobson header compression with its		
3156	foreign agent.		
3157	4.2.2. Foreign Agent Considerations		
3158	Upon receipt of an encapsulated datagram sent to its advertised		
3159	care-of address, a foreign agent MUST compare the inner destination		
3160	address to those entries in its visitor list. When the destination		
3161	does not match the address of any mobile node currently in the		
3162	visitor list, the foreign agent MUST NOT forward the datagram without		
3163	modifications to the original IP header, because otherwise a routing		
3164	loop is likely to result. The datagram SHOULD be silently discarded.		
3165	ICMP Destination Unreachable MUST NOT be sent when a foreign agent is		
3166	unable to forward an incoming tunneled datagram. Otherwise, the		
3167	foreign agent forwards the decapsulated datagram to the mobile node.		
3168	The foreign agent MUST NOT advertise to other routers in its routing		
3169	domain, nor to any other mobile node, the presence of a mobile router		
3170	(Section 4.5).		
3171	The foreign agent MUST route datagrams it receives from registered		
3172	mobile nodes. At a minimum, this means that the foreign agent must		
3173	verify the IP Header Checksum, decrement the IP Time To Live,		
3174	recompute the IP Header Checksum, and forward such datagrams to a		
3175	default router. In addition, the foreign agent SHOULD send an		
3176	appropriate ICMP Redirect message to the mobile node.		
3177			
3178			
3179			
3180			
3181			
3182			
3183			
3184			
3185			
3186			
3187			
3188			
3189			
3190			
3191			
3192			
3193			
3194	Perkins	Standards Track	[Page 57]

May 13 1998 10:38:26		rfc2002.txt	Page 58
3195	RFC 2002	IP Mobility Support	October 1996
3196			
3197			
3198			
3199	4.2.3. Home Agent Considerations		
3200			
3201	The home agent MUST be able to intercept any datagrams on the home		
3202	network addressed to the mobile node while the mobile node is		
3203	registered away from home. Proxy and gratuitous ARP MAY be used in		
3204	enabling this interception, as specified in Section 4.6.		
3205			
3206	The home agent must examine the IP Destination Address of all		
3207	arriving datagrams to see if it is equal to the home address of any		
3208	of its mobile nodes registered away from home. If so, the home agent		
3209	tunnels the datagram to the mobile node's currently registered care-		
3210	of address or addresses. If the home agent supports the optional		
3211	capability of multiple simultaneous mobility bindings, it tunnels a		
3212	copy to each care-of address in the mobile node's mobility binding		
3213	list. If the mobile node has no current mobility bindings, the home		
3214	agent MUST NOT attempt to intercept datagrams destined for the mobile		
3215	node, and thus will not in general receive such datagrams. However,		
3216	if the home agent is also a router handling common IP traffic, it is		
3217	possible that it will receive such datagrams for forwarding onto the		
3218	home network. In this case, the home agent MUST assume the mobile		
3219	node is at home and simply forward the datagram directly onto the		
3220	home network.		
3221			
3222	See Section 4.1 regarding methods of encapsulation that may be used		
3223	for tunneling. Nodes implementing tunneling SHOULD also implement		
3224	the "tunnel soft state" mechanism [14], which allows ICMP error		
3225	messages returned from the tunnel to correctly be reflected back to		
3226	the original senders of the tunneled datagrams.		
3227			
3228	Home agents SHOULD be able to decapsulate and further deliver packets		
3229	addressed to themselves, sent by a mobile node for the purpose of		
3230	maintaining location privacy, as described in Section 5.5.		
3231			
3232	If the Lifetime for a given mobility binding expires before the home		
3233	agent has received another valid Registration Request for that mobile		
3234	node, then that binding is deleted from the mobility binding list.		
3235	The home agent MUST NOT send any Registration Reply message simply		
3236	because the mobile node's binding has expired. The entry in the		
3237	visitor list of the mobile node's current foreign agent will expire		
3238	naturally, probably at the same time as the binding expired at the		
3239	home agent. When a mobility binding's lifetime expires, the home		
3240	agent MUST delete the binding, but it MUST retain any other (non-		
3241	expired) simultaneous mobility bindings that it holds for the mobile		
3242	node.		
3243			
3244			
3245	When a home agent receives a datagram, intercepted for one of its		
3246	mobile nodes registered away from home, the home agent MUST examine		
3247	the datagram to check if it is already encapsulated. If so, special		
3248			
3249	Perkins	Standards Track	[Page 58]

1251 RFC 2002 IP Mobility Support October 1996

1252

1253 rules apply in the forwarding of that datagram to the mobile node:

1254

1255

1256

1257 - If the inner (encapsulated) Destination Address is the same

1258 as the outer Destination Address (the mobile node), then the

1259 home agent MUST also examine the outer Source Address of the

1260 encapsulated datagram (the source address of the tunnel). If

1261 this outer Source Address is the same as the mobile node's

1262 current care-of address, the home agent MUST silently discard

1263 that datagram in order to prevent a likely routing loop. If,

1264 instead, the outer Source Address is NOT the same as the mobile

1265 node's current care-of address, then the home agent SHOULD

1266 forward the datagram to the mobile node. In order to forward

1267 the datagram in this case, the home agent MAY simply alter the

1268 outer Destination Address to the care-of address, rather than

1269 re-encapsulating the datagram.

1270

1271 - Otherwise (the inner Destination Address is NOT the same as the

1272 outer Destination Address), the home agent SHOULD encapsulate

1273 the datagram again (recursive encapsulation), with the new outer

1274 Destination Address set equal to the mobile node's care-of

1275 address. That is, the home agent forwards the entire datagram

1276 to the mobile node in the same way as any other datagram

1277 (encapsulated already or not).

1278

1279 4.3. Broadcast Datagrams

1280

1281 When a home agent receives a broadcast datagram, it MUST NOT forward

1282 the datagram to any mobile nodes in its mobility binding list other

1283 than those that have requested forwarding of broadcast datagrams. A

1284 mobile node MAY request forwarding of broadcast datagrams by setting

1285 the 'B' bit in its Registration Request message (Section 3.3). For

1286 each such registered mobile node, the home agent SHOULD forward

1287 received broadcast datagrams to the mobile node, although it is a

1288 matter of configuration at the home agent as to which specific

1289 categories of broadcast datagrams will be forwarded to such mobile

1290 nodes.

1291

1292 If the 'D' bit was set in the mobile node's Registration Request

1293 message, indicating that the mobile node is using a co-located care-

1294 of address, the home agent simply tunnels appropriate broadcast IP

1295 datagrams to the mobile node's care-of address. Otherwise (the 'D'

1296 bit was NOT set), the home agent first encapsulates the broadcast

1297 datagram in a unicast datagram addressed to the mobile node's home

1298 address, and then tunnels this encapsulated datagram to the foreign

1299 agent. This extra level of encapsulation is required so that the

1300 foreign agent can determine which mobile node should receive the

1301 datagram after it is decapsulated. When received by the foreign

1302 agent, the unicast encapsulated datagram is detunneled and delivered

1303

1304

1305

1306 Perkins Standards Track [Page 59]

3307 RFC 2002 IP Mobility Support October 1996

3308

3309

3310 to the mobile node in the same way as any other datagram. In either

3311 case, the mobile node must decapsulate the datagram it receives in

3312 order to recover the original broadcast datagram.

3313

3314 4.4. Multicast Datagram Routing

3315

3316 As mentioned previously, a mobile node that is connected to its home

3317 network functions in the same way as any other (fixed) host or

3318 router. Thus, when it is at home, a mobile node functions

3319 identically to other multicast senders and receivers. This section

3320 therefore describes the behavior of a mobile node that is visiting a

3321 foreign network.

3322

3323 In order to receive multicasts, a mobile node MUST join the multicast

3324 group in one of two ways. First, a mobile node MAY join the group

3325 via a (local) multicast router on the visited subnet. This option

3326 assumes that there is a multicast router present on the visited

3327 subnet. If the mobile node is using a co-located care-of address, it

3328 SHOULD use this address as the source IP address of its [CMP [5]]

3329 messages. Otherwise, it MUST use its home address.

3330

3331 Alternatively, a mobile node which wishes to receive multicasts MAY

3332 join groups via a bi-directional tunnel to its home agent, assuming

3333 that its home agent is a multicast router. The mobile node tunnels

3334 IGMP messages to its home agent and the home agent forwards multicast

3335 datagrams down the tunnel to the mobile node. The rules for

3336 multicast datagram delivery to mobile nodes in this case are

3337 identical to those for broadcast datagrams (Section 4.3). Namely, if

3338 the mobile node is using a co-located care-of address (the 'D' bit

3339 was set in the mobile node's Registration Request), then the home

3340 agent SHOULD tunnel the datagram to this care-of address; otherwise,

3341 the home agent MUST first encapsulate the datagram in a unicast

3342 datagram addressed to the mobile node's home address and then MUST

3343 tunnel the resulting datagram (recursive tunneling) to the mobile

3344 node's care-of address.

3345

3346 A mobile node that wishes to send datagrams to a multicast group also

3347 has two options: (1) send directly on the visited network; or (2)

3348 send via a tunnel to its home agent. Because multicast routing in

3349 general depends upon the IP source address, a mobile node which sends

3350 multicast datagrams directly on the visited network MUST use a co-

3351 located care-of address as the IP source address. Similarly, a

3352 mobile node which tunnels a multicast datagram to its home agent MUST

3353 use its home address as the IP source address of both the (inner)

3354 multicast datagram and the (outer) encapsulating datagram. This

3355 second option assumes that the home agent is a multicast router.

3356

3357

3358

3359

3360

3361 Perkins Standards Track [Page 60]

3362

3364 RFC 2002 IP Mobility Support October 1996
 3365
 3366
 3367 4.5. Mobile Routers
 3368
 3369 A mobile node can be a router, which is responsible for the mobility
 3370 of one or more entire networks moving together, perhaps on an
 3371 airplane, a ship, a train, an automobile, a bicycle, or a kayak. The
 3372 nodes connected to a network served by the mobile router may
 3373 themselves be fixed nodes or mobile nodes or routers. In this
 3374 document, such networks are called "mobile networks".
 3375
 3376 A mobile router MAY act as a foreign agent and provide a foreign
 3377 agent care-of address to mobile nodes connected to the mobile
 3378 network. Typical routing to a mobile node via a mobile router in
 3379 this case is illustrated by the following example:
 3380
 3381 a) A laptop computer is disconnected from its home network and
 3382 later attached to a network port in the seat back of an
 3383 aircraft. The laptop computer uses Mobile IP to register on
 3384 this foreign network, using a foreign agent care-of address
 3385 discovered through an Agent Advertisement from the aircraft's
 3386 foreign agent.
 3387
 3388 b) The aircraft network is itself mobile. Suppose the node
 3389 serving as the foreign agent on the aircraft also serves as
 3390 the default router that connects the aircraft network to the
 3391 rest of the Internet. When the aircraft is at home, this
 3392 router is attached to some fixed network at the airline's
 3393 headquarters, which is the router's home network. While
 3394 the aircraft is in flight, this router registers from time
 3395 to time over its radio link with a series of foreign agents
 3396 below it on the ground. This router's home agent is a node
 3397 on the fixed network at the airline's headquarters.
 3398
 3399 c) Some correspondent node sends a datagram to the laptop
 3400 computer, addressing the datagram to the laptop's home
 3401 address. This datagram is initially routed to the laptop's
 3402 home network.
 3403
 3404 d) The laptop's home agent intercepts the datagram on the home
 3405 network and tunnels it to the laptop's care-of address, which
 3406 in this example is an address of the node serving as router
 3407 and foreign agent on the aircraft. Normal IP routing will
 3408 route the datagram to the fixed network at the airline's
 3409 headquarters.
 3410
 3411
 3412
 3413
 3414
 3415
 3416
 3417
 3418 Perkins Standards Track [Page 61]

3419 RFC 2002 IP Mobility Support October 1996
 3420
 3421
 3422
 3423 e) The aircraft router and foreign agent's home agent there
 3424 intercepts the datagram and tunnels it to its current care-of
 3425 address, which in this example is some foreign agent on the
 3426 ground below the aircraft. The original datagram from the
 3427 correspondent node has now been encapsulated twice: once
 3428 by the laptop's home agent and again by the aircraft's home
 3429 agent.
 3430
 3431 f) The foreign agent on the ground decapsulates the datagram,
 3432 yielding a datagram still encapsulated by the laptop's home
 3433 agent, with a destination address of the laptop's care-of
 3434 address. The ground foreign agent sends the resulting
 3435 datagram over its radio link to the aircraft.
 3436
 3437 g) The foreign agent on the aircraft decapsulates the datagram,
 3438 yielding the original datagram from the correspondent node,
 3439 with a destination address of the laptop's home address.
 3440 The aircraft foreign agent delivers the datagram over the
 3441 aircraft network to the laptop's link-layer address.
 3442
 3443 This example illustrated the case in which a mobile node is attached
 3444 to a mobile network. That is, the mobile node is mobile with respect
 3445 to the network, which itself is also mobile (here with respect to the
 3446 ground). If, instead, the node is fixed with respect to the mobile
 3447 network (the mobile network is the fixed node's home network), then
 3448 either of two methods may be used to cause datagrams from
 3449 correspondent nodes to be routed to the fixed node.
 3450
 3451 A home agent MAY be configured to have a permanent registration for
 3452 the fixed node, that indicates the mobile router's address as the
 3453 fixed host's care-of address. The mobile router's home agent will
 3454 usually be used for this purpose. The home agent is then responsible
 3455 for advertising connectivity using normal routing protocols to the
 3456 fixed node. Any datagrams sent to the fixed node will thus use
 3457 recursive tunneling as described above.
 3458
 3459 Alternatively, the mobile router MAY advertise connectivity to the
 3460 entire mobile network using normal IP routing protocols through a
 3461 bi-directional tunnel to its own home agent. This method avoids the
 3462 need for recursive tunneling of datagrams.
 3463
 3464 4.6. ARP, Proxy ARP, and Gratuitous ARP
 3465
 3466 The use of ARP [16] requires special rules for correct operation when
 3467 wireless or mobile nodes are involved. The requirements specified in
 3468 this section apply to all home networks in which ARP is used for
 3469 address resolution.
 3470
 3471
 3472
 3473
 3474 Perkins Standards Track [Page 62]

3475 RPT 2002 IP Mobility Support October 1996
 3476
 3477
 3478
 3479 In addition to the normal use of ARP for resolving a target node's
 3480 link-layer address from its IP address, this document distinguishes
 3481 two special uses of ARP:
 3482
 3483 - A Proxy ARP [18] is an ARP Reply sent by one node on behalf
 3484 of another node which is either unable or unwilling to answer
 3485 its own ARP Requests. The sender of a Proxy ARP reverses the
 3486 Sender and Target Protocol Address fields as described in [16],
 3487 but supplies some configured link-layer address (generally, its
 3488 own) in the Sender Hardware Address field. The node receiving
 3489 the Reply will then associate this link-layer address with the
 3490 IP address of the original target node, causing it to transmit
 3491 future datagrams for this target node to the node with that
 3492 link-layer address.
 3493
 3494 - A Gratuitous ARP [23] is an ARP packet sent by a node in order to
 3495 spontaneously cause other nodes to update an entry in their ARP
 3496 cache. A gratuitous ARP MAY use either an ARP Request or an ARP
 3497 Reply packet. In either case, the ARP Sender Protocol Address
 3498 and ARP Target Protocol Address are both set to the IP address
 3499 of the cache entry to be updated, and the ARP Sender Hardware
 3500 Address is set to the link-layer address to which this cache
 3501 entry should be updated. When using an ARP Reply packet, the
 3502 Target Hardware Address is also set to the link-layer address to
 3503 which this cache entry should be updated (this field is not used
 3504 in an ARP Request packet).
 3505
 3506 In either case, for a gratuitous ARP, the ARP packet MUST be
 3507 transmitted as a local broadcast packet on the local link. As
 3508 specified in [16], any node receiving any ARP packet (Request or
 3509 Reply) MUST update its local ARP cache with the Sender Protocol
 3510 and Hardware Addresses in the ARP packet, if the receiving node
 3511 has an entry for that IP address already in its ARP cache. This
 3512 requirement in the ARP protocol applies even for ARP Request
 3513 packets, and for ARP Reply packets that do not match any ARP
 3514 Request transmitted by the receiving node [16].
 3515
 3516 While a mobile node is registered on a foreign network, its home
 3517 agent uses proxy ARP [18] to reply to ARP Requests it receives that
 3518 seek the mobile node's link-layer address. When receiving an ARP
 3519 Request, the home agent MUST examine the target IP address of the
 3520 Request, and if this IP address matches the home address of any
 3521 mobile node for which it has a registered mobility binding, the home
 3522 agent MUST transmit an ARP Reply on behalf of the mobile node. After
 3523 exchanging the sender and target addresses in the packet [18], the
 3524 home agent MUST set the sender link-layer address in the packet to
 3525 the link-layer address of its own interface over which the Reply will
 3526 be sent.
 3527
 3528
 3529
 3530 Perkins Standards Track [Page 63]

3531 RFC 2002 IP Mobility Support October 1996
 3532
 3533
 3534
 3535 When a mobile node leaves its home network and registers a binding on
 3536 a foreign network, its home agent uses gratuitous ARP to update the
 3537 ARP caches of nodes on the home network. This causes such nodes to
 3538 associate the link-layer address of the home agent with the mobile
 3539 node's home (IP) address. When registering a binding for a mobile
 3540 node for which the home agent previously had no binding (the mobile
 3541 node was assumed to be at home), the home agent MUST transmit a
 3542 gratuitous ARP on behalf of the mobile node. This gratuitous ARP
 3543 packet MUST be transmitted as a broadcast packet on the link on which
 3544 the mobile node's home address is located. Since broadcasts on the
 3545 local link (such as Ethernet) are typically not guaranteed to be
 3546 reliable, the gratuitous ARP packet SHOULD be retransmitted a small
 3547 number of times to increase its reliability.
 3548
 3549 When a mobile node returns to its home network, the mobile node
 3550 and its home agent use gratuitous ARP to cause all nodes on the
 3551 mobile node's home network to update their ARP caches to once again
 3552 associate the mobile node's own link-layer address with the mobile
 3553 node's home (IP) address. Before transmitting the (de)Registration
 3554 Request message to its home agent, the mobile node MUST transmit this
 3555 gratuitous ARP on its home network as a local broadcast on this link.
 3556 The gratuitous ARP packet SHOULD be retransmitted a small number of
 3557 times to increase its reliability, but these retransmissions SHOULD
 3558 proceed in parallel with the transmission and processing of its
 3559 (de)Registration Request.
 3560
 3561 When the mobile node's home agent receives and accepts this
 3562 (de)Registration Request, the home agent MUST also transmit a
 3563 gratuitous ARP on the mobile node's home network. This gratuitous
 3564 ARP also is used to associate the mobile node's home address with
 3565 the mobile node's own link-layer address. A gratuitous ARP is
 3566 transmitted by both the mobile node and its home agent, since in the
 3567 case of wireless network interfaces, the area within transmission
 3568 range of the mobile node will likely differ from that within range
 3569 of its home agent. The ARP packet from the home agent MUST be
 3570 transmitted as a local broadcast on the mobile node's home link,
 3571 and SHOULD be retransmitted a small number of times to increase
 3572 its reliability; these retransmissions, however, SHOULD proceed in
 3573 parallel with the transmission and processing of its (de)Registration
 3574 Reply.
 3575
 3576 While the mobile node is away from home, it MUST NOT transmit any
 3577 broadcast ARP Request or ARP Reply messages. Finally, while the
 3578 mobile node is away from home, it MUST NOT reply to ARP Requests
 3579 in which the target IP address is its own home address, unless the
 3580 ARP Request is sent by a foreign agent with which the mobile node
 3581 is attempting to register or a foreign agent with which the mobile
 3582 node has an unexpired registration. In the latter case, the mobile
 3583 node has an unexpired registration. In the latter case, the mobile
 3584 node has an unexpired registration. In the latter case, the mobile
 3585 node has an unexpired registration. In the latter case, the mobile
 3586 node has an unexpired registration. In the latter case, the mobile
 Perkins Standards Track [Page 64]

3587 RFC 2002 IP Mobility Support October 1996

3588

3589

3590

3591

3592

3593

3594

3595

3596

3597

3598

3599

3600

3601

3602

3603

3604

3605

3606

3607

3608

3609

3610

3611

3612

3613

3614

3615

3616

3617

3618

3619

3620

3621

3622

3623

3624

3625

3626

3627

3628

3629

3630

3631

3632

3633

3634

3635

3636

3637

3638

3639

3640

3641

3642

node MUST use a unicast ARP Reply to respond to the foreign agent. Note that if the mobile node is using a co-located care-of address and receives an ARP Request in which the target IP address is this care-of address, then the mobile node SHOULD reply to this ARP Request. Note also that, when transmitting a Registration Request on a foreign network, a mobile node may discover the link-layer address of a foreign agent by storing the address as it is received from the Agent Advertisement from that foreign agent, but not by transmitting a broadcast ARP Request message.

The specific order in which each of the above requirements for the use of ARP, proxy ARP, and gratuitous ARP are applied, relative to the transmission and processing of the mobile node's Registration Request and Registration Reply messages when leaving home or returning home, are important to the correct operation of the protocol.

To summarize the above requirements, when a mobile node leaves its home network, the following steps, in this order, MUST be performed:

- The mobile node decides to register away from home, perhaps because it has received an Agent Advertisement from a foreign agent and has not recently received one from its home agent.
- Before transmitting the Registration Request, the mobile node disables its own future processing of any ARP Requests it may subsequently receive requesting the link-layer address corresponding to its home address, except insofar as necessary to communicate with foreign agents on visited networks.
- The mobile node transmits its Registration Request.
- When the mobile node's home agent receives and accepts the Registration Request, it performs a gratuitous ARP on behalf of the mobile node, and begins using proxy ARP to reply to ARP Requests that it receives requesting the mobile node's link-layer address. If, instead, the home agent rejects the Registration Request, no ARP processing (gratuitous nor proxy) is performed by the home agent.

When a mobile node later returns to its home network, the following steps, in this order, MUST be performed:

- The mobile node decides to register at home, perhaps because it has received an Agent Advertisement from its home agent.

Standards Track

(Page 65)

Perkins

3643 RFC 2002 IP Mobility Support October 1996

3644

3645

3646

3647

3648

3649

3650

3651

3652

3653

3654

3655

3656

3657

3658

3659

3660

3661

3662

3663

3664

3665

3666

3667

3668

3669

3670

3671

3672

3673

3674

3675

3676

3677

3678

3679

3680

3681

3682

3683

3684

3685

3686

3687

3688

3689

3690

3691

3692

3693

3694

3695

3696

3697

3698

- Before transmitting the Registration Request, the mobile node re-enables its own future processing of any ARP Requests it may subsequently receive requesting its link-layer address.
- The mobile node performs a gratuitous ARP for itself.
- The mobile node transmits its Registration Request.
- When the mobile node's home agent receives and accepts the Registration Request, it stops using proxy ARP to reply to ARP Requests that it receives requesting the mobile node's link-layer address, and then performs a gratuitous ARP on behalf of the mobile node. If, instead, the home agent rejects the Registration Request, no ARP processing (gratuitous nor proxy) is performed by the home agent.

5. Security Considerations

The mobile computing environment is potentially very different from the ordinary computing environment. In many cases, mobile computers will be connected to the network via wireless links. Such links are particularly vulnerable to passive eavesdropping, active replay attacks, and other active attacks.

5.1. Message Authentication Codes

Home agents and mobile nodes MUST be able to perform authentication. The default algorithm is keyed MD5 [21], with a key size of 128 bits. The default mode of operation is to both precede and follow the data to be hashed, by the 128-bit key; that is, MD5 is to be used in "prefix-suffix" mode. The foreign agent MUST also support authentication using keyed MD5 and key sizes of 128 bits or greater, with manual key distribution. More authentication algorithms, algorithm modes, key distribution methods, and key sizes MAY also be supported.

5.2. Areas of Security Concern in this Protocol

The registration protocol described in this document will result in a mobile node's traffic being tunneled to its care-of address. This tunneling feature could be a significant vulnerability if the registration were not authenticated. Such remote redirection, for instance as performed by the mobile registration protocol, is widely understood to be a security problem in the current Internet if not authenticated [2]. Moreover, the Address Resolution Protocol (ARP) is not authenticated, and can potentially be used to steal another host's traffic. The use of "Gratuitous ARP" (Section 4.6) brings with it all of the risks associated with the use of ARP.

Standards Track

(Page 66)

Perkins

3699 RFC 2002 IP Mobility Support October 1996
 3700
 3701
 3702
 3703 5.3. Key Management
 3704
 3705 This specification requires a strong authentication mechanism (keyed
 3706 MD5) which precludes many potential attacks based on the Mobile IP
 3707 registration protocol. However, because key distribution is
 3708 difficult in the absence of a network key management protocol,
 3709 messages with the foreign agent are not all required to be
 3710 authenticated. In a commercial environment it might be important to
 3711 authenticate all messages between the foreign agent and the home
 3712 agent, so that billing is possible, and service providers do not
 3713 provide service to users that are not legitimate customers of that
 3714 service provider.
 3715

5.4. Picking Good Random Numbers

3716
 3717 The strength of any authentication mechanism depends on several
 3718 factors, including the innate strength of the authentication
 3719 algorithm, the secrecy of the key used, the strength of the key used,
 3720 and the quality of the particular implementation. This specification
 3721 requires implementation of keyed MD5 for authentication, but does not
 3722 preclude the use of other authentication algorithms and modes. For
 3723 keyed MD5 authentication to be useful, the 128-bit key must be both
 3724 secret (that is, known only to authorized parties) and pseudo-random.
 3725 If nonces are used in connection with replay protection, they must
 3726 also be selected carefully. Eastlake, et al. [7] provides more
 3727 information on generating pseudo-random numbers.
 3728

5.5. Privacy

3729
 3730 Users who have sensitive data that they do not wish others to see
 3731 should use mechanisms outside the scope of this document (such as
 3732 encryption) to provide appropriate protection. Users concerned about
 3733 traffic analysis should consider appropriate use of link encryption.
 3734 If absolute location privacy is desired, the mobile node can create a
 3735 tunnel to its home agent. Then, datagrams destined for correspondent
 3736 nodes will appear to emanate from the home network, and it may be
 3737 more difficult to pinpoint the location of the mobile node. Such
 3738 mechanisms are all beyond the scope of this document.
 3739
 3740
 3741
 3742
 3743
 3744
 3745
 3746
 3747
 3748
 3749
 3750
 3751
 3752
 3753

3755 EFC 2002 IP Mobility Support October 1996
 3756
 3757
 3758

5.6. Replay Protection for Registration Requests

3759
 3760 The Identification field is used to let the home agent verify that a
 3761 registration message has been freshly generated by the mobile node,
 3762 not replayed by an attacker from some previous registration. Two
 3763 methods are described in this section: timestamps (mandatory) and
 3764 "nonces" (optional). All mobile nodes and home agents MUST implement
 3765 timestamp-based replay protection. These nodes MAY also implement
 3766 nonce-based replay protection (but see Appendix A.2 for a patent that
 3767 may apply to nonce-based replay protection).
 3768

3769
 3770 The style of replay protection in effect between a mobile node and
 3771 its home agent is part of the mobile security association. A mobile
 3772 node and its home agent MUST agree on which method of replay
 3773 protection will be used. The interpretation of the Identification
 3774 field depends on the method of replay protection as described in the
 3775 subsequent subsections.
 3776

3777 Whatever method is used, the low-order 32 bits of the Identification
 3778 MUST be copied unchanged from the Registration Request to the Reply.
 3779 The foreign agent uses those bits (and the mobile node's home
 3780 address) to match Registration Requests with corresponding replies.
 3781 The mobile node MUST verify that the low-order 32 bits of any
 3782 Registration Reply are identical to the bits it sent in the
 3783 Registration Request.
 3784

3785 The Identification in a new Registration Request MUST NOT be the same
 3786 as in an immediately preceding Request, and SHOULD NOT repeat while
 3787 the same security context is being used between the mobile node and
 3788 the home agent. Retransmission as in Section 3.6.3 is allowed.
 3789

5.6.1. Replay Protection using Timestamps

3790
 3791 The basic principle of timestamp replay protection is that the node
 3792 generating a message inserts the current time of day, and the node
 3793 receiving the message checks that this timestamp is sufficiently
 3794 close to its own time of day. Obviously the two nodes must have
 3795 adequately synchronized time-of-day clocks. As with any messages,
 3796 time synchronization messages may be protected against tampering by
 3797 an authentication mechanism determined by the security context
 3798 between the two nodes.
 3799
 3800

3801 If timestamps are used, the mobile node MUST set the Identification
 3802 field to a 64-bit value formatted as specified by the Network Time
 3803 Protocol [13]. The low-order 32 bits of the NTP format represent
 3804 fractional seconds, and those bits which are not available from a
 3805 time source SHOULD be generated from a good source of randomness.
 3806 Note, however, that when using timestamps, the 64-bit Identification
 3807
 3808
 3809
 3810

3811 RFC: 2002 IP Mobility Support October 1996

3812

3813

3814

3815 used in a Registration Request from the mobile node MUST be greater

3816 than that used in any previous Registration Request, as the home

3817 agent uses this field also as a sequence number. Without such a

3818 sequence number, it would be possible for a delayed duplicate of an

3819 earlier Registration Request to arrive at the home agent (within the

3820 clock synchronization required by the home agent), and thus be

3821 applied out of order, mistakenly altering the mobile node's current

3822 registered care-of address.

3823

3824 Upon receipt of a Registration Request with a valid Mobile-Home

3825 Authentication Extension, the home agent MUST check the

3826 Identification field for validity. In order to be valid, the

3827 timestamp contained in the Identification field MUST be close enough

3828 to the home agent's time of day clock and the timestamp MUST be

3829 greater than all previously accepted timestamps for the requesting

3830 mobile node. Time tolerances and resynchronization details are

3831 specific to a particular mobility security association.

3832

3833 If the timestamp is valid, the home agent copies the entire

3834 Identification field into the Registration Reply it returns the Reply

3835 to the mobile node. If the timestamp is not valid, the home agent

3836 copies only the low-order 32 bits into the Registration Reply, and

3837 supplies the high-order 32 bits from its own time of day. In this

3838 latter case, the home agent MUST reject the registration by returning

3839 Code 133 (identification mismatch) in the Registration Reply.

3840

3841 As described in Section 3.6.2.1, the mobile node MUST verify that the

3842 low-order 32 bits of the Identification in the Registration Reply are

3843 identical to those in the rejected registration attempt, before using

3844 the high-order bits for clock resynchronization.

3845

3846 5.6.2. Replay Protection using Nonces

3847 Implementors of this optional mechanism should examine Appendix A.2

3848 for a patent that may be applicable to nonce-based replay protection.

3849

3850

3851 The basic principle of nonce replay protection is that node A

3852 includes a new random number in every message to node B, and checks

3853 that node B returns that same number in its next message to node A.

3854 Both messages use an authentication code to protect against

3855 alteration by an attacker. At the same time node B can send its own

3856 nonces in all messages to node A (to be echoed by node A), so that it

3857 too can verify that it is receiving fresh messages.

3858

3859 The home agent may be expected to have resources for computing

3860 pseudo-random numbers useful as nonces [7]. It inserts a new nonce

3861 as the high-order 32 bits of the identification field of every

3862 Registration Reply. The home agent copies the low-order 32 bits of

3863

3864

3865

3866

Perkins

Standards Track

[Page 69]

3867 RFC: 2002 IP Mobility Support October 1996

3868

3869

3870

3871 the Identification from the Registration Request message into the

3872 low-order 32 bits of the Identification in the Registration Reply.

3873 When the mobile node receives an authenticated Registration Reply

3874 from the home agent, it saves the high-order 32 bits of the

3875 identification for use as the high-order 32 bits of its next

3876 Registration Request.

3877

3878 The mobile node is responsible for generating the low-order 32 bits

3879 of the Identification in each Registration Request. Ideally it

3880 should generate its own random nonces. However it may use any

3881 expedient method, including duplication of the random value sent by

3882 the home agent. The method chosen is of concern only to the mobile

3883 node, because it is the node that checks for valid values in the

3884 Registration Reply. The high-order and low-order 32 bits of the

3885 identification chosen SHOULD both differ from their previous values.

3886 The home agent uses a new high-order value and the mobile node uses a

3887 new low-order value for each registration message. The foreign agent

3888 uses the low-order value (and the mobile host's home address) to

3889 correctly match registration replies with pending Requests (Section

3890 3.7.1).

3891

3892 If a registration message is rejected because of an invalid nonce,

3893 the Reply always provides the mobile node with a new nonce to be used

3894 in the next registration. Thus the nonce protocol is self-

3895 synchronizing.

3896

3897

3898

3899

3900

3901

3902

3903

3904

3905

3906

3907

3908

3909

3910

3911

3912

3913

3914

3915

3916

3917

3918

3919

3920

3921

3922

Perkins

Standards Track

[Page 70]

1924 RFC 2002 IP Mobility Support October 1996
 1925
 1926
 1927 6. Acknowledgments

1928 Special thanks to Steve Deering (Xerox PARC), along with Dan Duchamp
 1929 and John Iounidis (JJI) (Columbia), for forming the working group,
 1930 chairing it, and putting so much effort into its early development.
 1931
 1932

1933 Thanks also to Kannan Alagappan, Greg Minshall, and Tony Li for their
 1934 contributions to the group while performing the duties of
 1935 chairperson, as well as for their many useful comments.
 1936

1937 Thanks to the active members of the Mobile IP Working Group,
 1938 particularly those who contributed text, including (in alphabetical
 1939 order)

- Ran Atkinson (Naval Research Lab),
- Dave Johnson (Carnegie Mellon University),
- Frank Kastenholz (FTP Software),
- Anders Klemets (KTH),
- Chip Maguire (KTH),
- Andrew Hylles (Macquarie University),
- Al Qurt (Bell Northern Research),
- Yakov Rekhter (IBM), and
- Fumio Teraoka (Sony).

1940
 1941 Thanks to Charlie Kunzinger and to Bill Simpson, the editors who
 1942 produced the first drafts for of this document, reflecting the
 1943 discussions of the Working Group. Much of the new text of this memo
 1944 is due to Jim Solomon and Dave Johnson.

1945
 1946 Thanks to Greg Minshall (Novell), Phil Karn (Qualcomm), and Frank
 1947 Kastenholz (FTP Software) for their generous support in hosting
 1948 interim Working Group meetings.

1949
 1950
 1951
 1952
 1953
 1954
 1955
 1956
 1957
 1958
 1959
 1960
 1961
 1962
 1963
 1964
 1965
 1966
 1967
 1968
 1969
 1970
 1971
 1972
 1973
 1974
 1975
 1976
 1977

Perkins Standards Track (Page 71)

3979 RFC 2002 IP Mobility Support October 1996
 3980
 3981
 3982
 3983 A. Patent Issues
 3984

3985 As of the time of publication, the IETF had been made aware of two
 3986 patents that may be relevant to implementors of the protocol
 3987 described in this technical specification.
 3988

3989 A.1. IBM Patent #5,159,592
 3990
 3991 Charles Perkins, editor of this memo, is sole inventor of U.S. Patent
 3992 No. 5,159,592, assigned to IBM. In a letter dated May 30, 1995, IBM
 3993 brought this patent to the attention of the IETF, stating that this
 3994 patent "relates to the Mobile IP." We understand that IBM did not
 3995 intend to assert that any particular implementation of Mobile IP
 3996 would or would not infringe the patent, but rather that IBM was
 3997 meeting what it viewed as a duty to disclose information that could
 3998 be relevant to the process of adopting a standard.
 3999

4000 Based on a review of the claims of the patent, IETF believes that a
 4001 system of registering an address obtained from a foreign agent, as
 4002 described in the document, would not necessarily infringe any of the
 4003 claims of the patent; and that a system in which an address is
 4004 obtained elsewhere and then registered can be implemented without
 4005 necessarily infringing any claims of the patent. Accordingly, our
 4006 view is that the proposed protocol can be implemented without
 4007 necessarily infringing the Perkins Patent.
 4008

4009 Parties considering adopting this protocol must be aware that some
 4010 specific implementations, or features added to otherwise non-
 4011 infringing implementations, may raise an issue of infringement with
 4012 respect to this patent or to some other patent.
 4013

4014 This statement is for the IETF's assistance in its standard-setting
 4015 procedure, and should not be relied upon by any party as an opinion
 4016 or guarantee that any implementation it might make or use would not
 4017 be covered by the Perkins Patent and any other patents. In
 4018 particular, IBM might disagree with the interpretation of this patent
 4019 described herein.
 4020

4021 A.2. IBM Patent #5,148,479
 4022

4023 This patent, also assigned to IBM, may be relevant to those who
 4024 implement nonce-based replay protection as described in Section
 4025 5.6.2. Note that nonce-based replay protection is an optional
 4026 feature of this specification. Timestamp-based replay protection, on
 4027 the other hand, (Section 5.6.1) is a requirement of this
 4028 specification.
 4029
 4030
 4031
 4032
 4033
 4034

Perkins Standards Track (Page 72)

May 13 1998 10:38:26

rfc2002.txt

Page 73

4015 RFC 2002 IP Mobility Support October 1996

4016

4017

4018

4019 B. Link-Layer Considerations

4020

4021 The mobile node MAY use link-layer mechanisms to decide that its

4022 point of attachment has changed. Such indications include the

4023 Down/Testing/Up interface status [11], and changes in cell or

4024 administration. The mechanisms will be specific to the particular

4025 link-layer technology, and are outside the scope of this document.

4026

4027 The Point-to-Point-Protocol (PPP) [22] and its Internet Protocol

4028 Control Protocol (IPCP) [12], negotiates the use of IP addresses.

4029

4030 The mobile node SHOULD first attempt to specify its home address, so

4031 that if the mobile node is attaching to its home network, the

4032 unrouted link will function correctly. When the home address is not

4033 accepted by the peer, but a transient IP address is dynamically

4034 assigned to the mobile node, and the mobile node is capable of

4035 supporting a co-located care-of address, the mobile node MAY register

4036 that address as a co-located care-of address. When the peer

4037 specifies its own IP address, that address MUST NOT be assumed to be

4038 a foreign agent care-of address or the IP address of a home agent.

4039

4040 C. TCP Considerations

4041

4042 C.1. TCP Timers

4043

4044 Most hosts and routers which implement TCP/IP do not permit easy

4045 configuration of the TCP timer values. When high-delay (e.g.,

4046 SATCOM) or low-bandwidth (e.g., High-Frequency Radio) links are in

4047 use, the default TCP timer values in many systems may cause

4048 retransmissions or timeouts, even when the link and network are

4049 actually operating properly with greater than usual delays because of

4050 the medium in use. This can cause an inability to create or maintain

4051 TCP connections over such links, and can also cause unwanted

4052 retransmissions which consume already scarce bandwidth. Vendors are

4053 encouraged to make TCP timers more configurable. Vendors of systems

4054 designed for the mobile computing markets should pick default timer

4055 values more suited to low-bandwidth, high-delay links. Users of

4056 mobile nodes should be sensitive to the possibility of timer-related

4057 difficulties.

4058

4059 C.2. TCP Congestion Management

4060

4061 Mobile nodes often use media which are more likely to introduce

4062 errors, effectively causing more packets to be dropped. This

4063 introduces a conflict with the mechanisms for congestion management

4064 found in modern versions of TCP [9]. Now, when a packet is dropped,

4065 the correspondent node's TCP implementation is likely to react as if

4066 there were a source of network congestion, and initiate the slow-

4067

4068

4069

4070

4071

4072

4073

4074

4075

4076

4077

4078

4079

4080

4081

4082

4083

4084

4085

4086

4087

4088

4089

4090

Perkins

Standards Track

[Page 73]

May 13 1998 10:38:26	rfc2002.txt	Page 74
4091	RFC 2002	October 1996
4092	IP Mobility Support	
4093		
4094		
4095	start mechanisms [9] designed for controlling that problem. However,	
4096	those mechanisms are inappropriate for overcoming errors introduced	
4097	by the links themselves, and have the effect of magnifying the	
4098	discontinuity introduced by the dropped packet. This problem has	
4099	been analyzed by Caceres, et al. [3]; there is no easy solution	
4100	available, and certainly no solution likely to be installed soon on	
4101	all correspondent nodes. While this problem is beyond the scope of	
4102	this document, it does illustrate that providing performance	
4103	transparency to mobile nodes involves understanding mechanisms	
4104	outside the network layer. It also indicates the need to avoid	
4105	designs which systematically drop packets; such designs might	
4106	otherwise be considered favorably when making engineering tradeoffs.	
4107		
4108	D. Example Scenarios	
4109		
4110	This section shows example Registration Requests for several common	
4111	scenarios.	
4112		
4113	D.1. Registering with a Foreign Agent Care-of Address	
4114		
4115	The mobile node receives an Agent Advertisement from a foreign agent	
4116	and wishes to register with that agent using the advertised foreign	
4117	agent care-of address. The mobile node wishes only IP-in-IP	
4118	encapsulation, does not want broadcasts, and does not want	
4119	simultaneous mobility bindings:	
4120		
4121	IP fields:	
4122	Source Address = mobile node's home address	
4123	Destination Address = copied from the IP source address of the	
4124	Agent Advertisement	
4125	Time to live = 1	
4126	UDP fields:	
4127	Source Port = <any>	
4128	Destination Port = 434	
4129	Registration Request fields:	
4130	Type = 1	
4131	S=0, B=0, D=0, M=0, G=0	
4132	Lifetime = the Registration Lifetime copied from the	
4133	Mobility Agent Advertisement Extension of the	
4134	Router Advertisement message	
4135	Home Address = the mobile node's home address	
4136	Home Agent = IP address of mobile node's home agent	
4137	Care-of Address = the Care-of Address copied from the	
4138	Mobility Agent Advertisement Extension of the	
4139	Router Advertisement message	
4140	Identification = Network Time Protocol timestamp or Nonce	
4141	Extensions:	
4142	The Mobile-Home Authentication Extension	
4143		
4144		
4145		
4146	Perkins	Standards Track [Page 74]

May 13 1998 10:38:26		rfc2002.txt	Page 75
4147	RFC 2002	IP Mobility Support	October 1996
4148			
4149			
4150			
4151		D.2. Registering with a Co-Located Care-of Address	
4152			
4153		The mobile node enters a foreign network that contains no foreign	
4154		agents. The mobile node obtains an address from a DHCP server [6]	
4155		for use as a co-located care-of address. The mobile node supports	
4156		all forms of encapsulation (IP-in-IP, minimal encapsulation, and	
4157		GRE), desires a copy of broadcast datagrams on the home network, and	
4158		does not want simultaneous mobility bindings:	
4159			
4160		IP fields:	
4161		Source Address = care-of address obtained from DHCP server	
4162		Destination Address = IP address of home agent	
4163		Time to Live = 64	
4164		UDP fields:	
4165		Source Port = <any>	
4166		Destination Port = 434	
4167		Registration Request fields:	
4168		Type = 1	
4169		S=0, B=1, D=1, M=1, G=1	
4170		Lifetime = 1800 (seconds)	
4171		Home Address = the mobile node's home address	
4172		Home Agent = IP address of mobile node's home agent	
4173		Care-of Address = IP address of address obtained from DHCP server	
4174		Identification = Network Time Protocol timestamp or Nonce	
4175		Extensions:	
4176		The Mobile-Home Authentication Extension	
4177			
4178			
4179			
4180			
4181			
4182			
4183			
4184			
4185			
4186			
4187			
4188			
4189			
4190			
4191			
4192			
4193			
4194			
4195			
4196			
4197			
4198			
4199			
4200			
4201	Perkins		
4202		Standards Track	[Page 75]

May 13 1998 10:38:26		rfc2002.txt	Page 76
4203	RFC 2002	IP Mobility Support	October 1996
4204			
4205			
4206			
4207		D.3. Deregistration	
4208			
4209		The mobile node returns home and wishes to deregister all care-of	
4210		addresses with its home agent.	
4211			
4212		IP fields:	
4213		Source Address = mobile node's home address	
4214		Destination Address = IP address of home agent	
4215		Time to Live = 1	
4216		UDP fields:	
4217		Source Port = <any>	
4218		Destination Port = 434	
4219		Registration Request fields:	
4220		Type = 1	
4221		S=0, B=0, D=0, M=0, G=0	
4222		Lifetime = 0	
4223		Home Address = the mobile node's home address	
4224		Home Agent = IP address of mobile node's home agent	
4225		Care-of Address = the mobile node's home address	
4226		Identification = Network Time Protocol timestamp or Nonce	
4227		Extensions:	
4228		The Mobile-Home Authentication Extension	
4229			
4230		E. Applicability of Prefix Lengths Extension	
4231			
4232		Caution is indicated with the use of the Prefix Lengths Extension	
4233		over wireless links, due to the irregular coverage areas provided by	
4234		wireless transmitters. As a result, it is possible that two foreign	
4235		agents advertising the same prefix might indeed provide different	
4236		connectivity to prospective mobile nodes. The Prefix-lengths	
4237		Extension SHOULD NOT be included in the advertisements sent by agents	
4238		in such a configuration.	
4239			
4240			
4241			
4242			
4243			
4244			
4245			
4246			
4247			
4248			
4249			
4250			
4251			
4252			
4253			
4254			
4255			
4256			
4257	Perkins		
4258		Standards Track	[Page 76]

May 13 1998 10:38:26		rfc2002.txt	Page 77
4259	RFC 2002	IP Mobility Support	October 1996
4260		Foreign agents using different wireless interfaces would have to cooperate using special protocols to provide identical coverage in space, and thus be able to claim to have wireless interfaces situated on the same subnetwork. In the case of wired interfaces, a mobile node disconnecting and subsequently connecting to a new point of attachment, may well send in a new Registration Request no matter whether the new advertisement is on the same medium as the last recorded advertisement. And, finally, in areas with dense populations of foreign agents it would seem unwise to require the propagation via routing protocols of the subnet prefixes associated with each individual wireless foreign agent; such a strategy could lead to quick depletion of available space for routing tables. Unwarranted increases in the time required for processing routing updates, and longer decision times for route selection if routes (which are almost always unnecessary) are stored for wireless "subnets".	
4261		References	
4262		[1] Atkinson, R., "IP Authentication Header", RFC 1826, August 1995.	
4263		[2] S. M. Bellovin, "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communications Review, 19(2), March 1989.	
4264		[3] Ramon Caceres and Liviu Iftode, "Improving the Performance of Reliable Transport Protocols in Mobile Computing Environments", IEEE Journal on Selected Areas in Communications, 13(5):850--857, June 1995.	
4265		[4] Deering, S., Editor, "ICMP Router Discovery Messages", RFC 1256, September 1991.	
4266		[5] Deering, S., "Host Extensions for IP Multicasting", STD 5, RFC 1112, August 1989.	
4267		[6] Drums, R., "Dynamic Host Configuration Protocol", RFC 1541, October 1993.	
4268		[7] Eastlake, D., Crocker, S., and J. Schiller, "Randomness Requirements for Security", RFC 1750, December 1994.	
4269		[8] Hanks, S., Li, R., Farinacci, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 1701, October 1994.	
4270		[9] Van Jacobson, "Congestion Avoidance and Control", In Proceedings of the SIGCOMM '88 Symposium: Communications Architectures & Protocols, pages 314--329, August 1988.	
4271		Perkins	Standards Track (Page 77)
4272		4314	

May 13 1998 10:38:26		rfc2002.txt	Page 78
4315	RFC 2002	IP Mobility Support	October 1996
4316		[10] Jacobson, V., "Compressing TCP/IP Headers for Low-Speed Serial Links", RFC 1144, February 1990.	
4317		[11] McCloghrie, K., and F. Kastenholz, "Evolution of the Interfaces Group of MIB-II", RFC 1573, January 1994.	
4318		[12] McGregor, G., "The PPP Internet Protocol Control Protocol (IPCP)", RFC 1332, May 1992.	
4319		[13] Mills, D., "Network Time Protocol (Version 3): Specification, Implementation and Analysis", RFC 1305, March 1992.	
4320		[14] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.	
4321		[15] Perkins, C., "Minimal Encapsulation within IP", RFC 2004, October 1996.	
4322		[16] Plummer, D., "An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48-bit Ethernet Addresses for Transmission on Ethernet Hardware", STD 37, RFC 826, November 1982.	
4323		[17] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.	
4324		[18] Postel, J., "Multi-LAN Address Resolution", RFC 925, October 1984.	
4325		[19] Postel, J., Editor, "Internet Protocol", STD 5, RFC 791, September 1981.	
4326		[20] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1700, October 1994.	
4327		[21] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.	
4328		[22] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.	
4329		[23] W. Richard Stevens, "TCP/IP Illustrated, Volume 1: The Protocols", Addison-Wesley, Reading, Massachusetts, 1994.	
4330		Perkins	Standards Track (Page 78)
4331		4370	

4371 RFC 2002 IP Mobility Support October 1996

4372 Editor's Address

4373 Questions about this memo can also be directed to the editor:

4374 Charles Perkins

4375 Room H3-D14

4376 T. J. Watson Research Center

4377 IBM Corporation

4378 30 Saw Mill River Rd.

4379 Hawthorne, NY 10532

4380 Work: +1-914-784-7350

4381 Fax: +1-914-784-6205

4382 Email: perk@watson.ibm.com

4383

4384 The working group can be contacted via the current chair:

4385 Jim Solomon

4386 Motorola, Inc.

4387 1301 E. Algonquin Rd.

4388 Schaumburg, IL 60196

4389 Work: +1-847-576-2753

4390 Email: solomon@comm.mot.com

4391

4392

4393

4394

4395

4396

4397

4398

4399

4400

4401

4402

4403

4404

4405

4406

4407

4408

4409

4410

4411

4412

4413

4414

4415

4416

4417

4418

4419

4420

4421

4422

4423

4424

4425

4426

[Page 79]

Standards Track

4427